Method and device for protecting digital data by double re-encryption

Patent number: CN1330819
Publication date: 2002-01-09
Inventor: MAKOTO SAITO (JP)
Applicant: MITSUBISHI CORP (JP)
Classification:
- international: H04L9/14; G11B20/10; H04N71/67; G06F17/60
- european:
Application number: CN19990814510 19991015
Priority number(s): JP19980309418 19981015

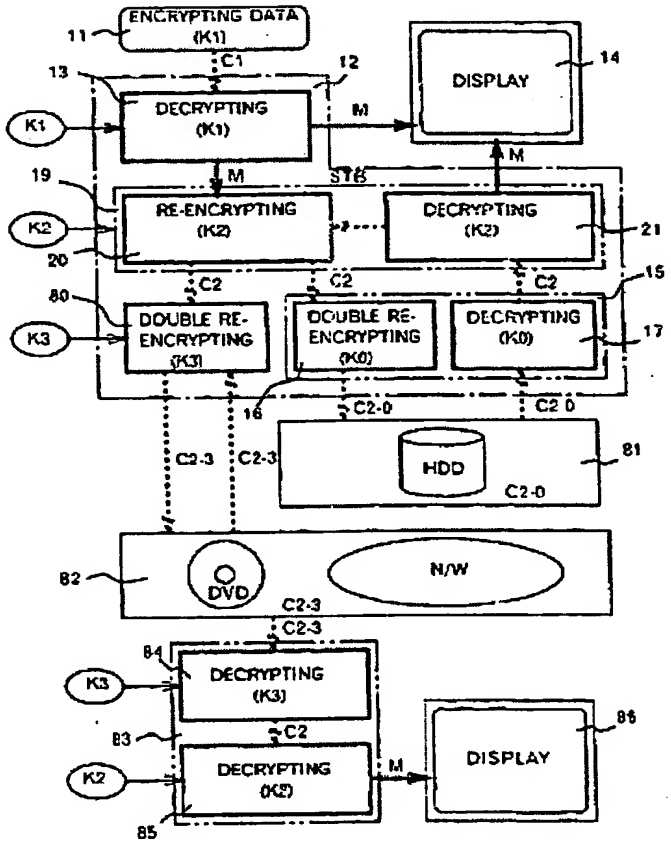
Also published as:
EP1122910 (A1)
WO0022777 (A1)
JP2002101089 (A)
CA2347480 (A1)

Report a data error here

Abstract not available for CN1330819
Abstract of corresponding document: **EP1122910**

A method and an apparatus allowing to ensure protecting digital data are provided. In addition to re-encrypting the data by using an unchangeable key, the data is double re-encrypted by using a changeable key. The changeable key is used first and the unchangeable key is then used, or in another case, the unchangeable key is used first, and the changeable key is then used. In the aspect of embodiments, there is a case adopting a software, a case adopting a hardware, or a case adopting the software and the hardware in combination. The hardware using the unchangeable key developed for digital video is available. In adopting the software, encryption/decryption is performed in a region below the kernel where the user cannot handle to ensure the security for the program and for the key used. More concretely, encryption/decryption is performed in a filter driver, a device driver, i.e., a disk driver and a network driver, in an I/O manager and an RTOS using a HAL. Either one of two filter drivers, with a file system driver between them, may be used and further, both of them may be used.

FIG. 8



[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/14
G11B 20/10 H04N 7/167
G06F 17/60

[12]发明专利申请公开说明书

[21]申请号 99814510.6

[43]公开日 2002年1月9日

[11]公开号 CN 1330819A

[22]申请日 1999.10.15 [21]申请号 99814510.6
[30]优先权
[32]1998.10.15 [33]JP [31]309418/1998
[86]国际申请 PCT/JP99/05704 1999.10.15
[87]国际公布 WO00/22777 日 2000.4.20
[85]进入国家阶段日期 2001.6.15
[71]申请人 三菱商事株式会社
地址 日本东京都
[72]发明人 齐藤诚

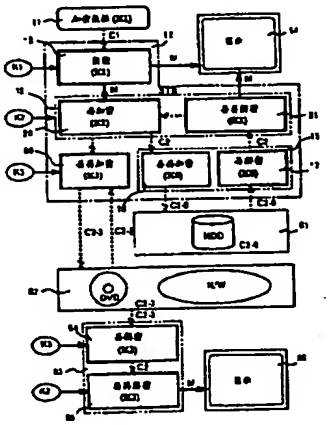
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 刘宗杰 王忠忠

权利要求书13页 说明书34页 附图页数14页

[54]发明名称 利用双重加密保护数字数据的方法及装置

[57]摘要

一种能可靠地保护数字数据的方法及装置。在使用固定密钥再加密的基础上使用可变密钥进行双重再加密。按密码密钥的使用顺序来分,有开始使用可变密钥其次使用固定 密钥的情况和开始使用固定密钥其次使用可变密钥的情况。作为实施 形态有利用软件和利用硬件的情况,进而还有软硬件组合的情况。作 为硬件,可以利用面向数字图像开发的使用固定密钥的硬件。为了保 证利用软件时的程序和使用的密钥的安全性,在用户不能利用的核心 部以下的区域进行加密/解密。具体地说,在I/O管理程序内的设备 驱动程序、即滤波驱动程序、盘驱动/网络驱动程序和利用HAL的RTOS中进行加密/解密。滤波驱动程序有2个,将文件系统驱动程序夹在 中间,利用哪一个都行,也可以2个都利用。



ISSN1008-4274

01.06.15

权 利 要 求 书

1. 一种对已将加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护方法，其特征在于：上述数字数据保护方法具有：

使用可变密钥对上述解密数字数据进行加密并将其作为可变密钥再加密数字数据的过程；

为了保存、复制或转送上述可变密钥再加密数字数据利用使用装置内藏的固定密钥进行加密并将其作为固定密钥一可变密钥双重再加密数字数据的过程；

使用上述固定密钥对保存、复制或转送的上述固定密钥一可变密钥双重再加密数字数据进行解密并将其作为可变密钥再加密数字数据的过程；

使用上述可变密钥对上述可变密钥再加密数字数据进行解密并将其作为上述解密数字数据的过程。

2. 一种对已将加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护方法，其特征在于：上述数字数据保护方法具有：

利用使用装置内藏的固定密钥对上述解密数字数据进行加密并将其作为固定密钥再加密数字数据的过程；

为了保存、复制或转送上述固定密钥再加密数字数据使用可变密钥对上述固定密钥再加密数字数据进行加密并将其作为固定密钥一可变密钥双重再加密数字数据的过程；

使用上述可变密钥对保存、复制或转送的上述固定密钥一可变密钥双重再加密数字数据进行解密并将其作为可变密钥再加密数字数据的过程；

使用上述固定密钥对上述可变密钥再加密数字数据进行解密并将其作为上述解密数字数据的过程。

3. 权利要求 1 或权利要求 2 的数字数据保护方法，其特征在于：使用上述可变密钥的加密和解密利用软件进行。

4. 权利要求 1 或权利要求 2 的数字数据保护方法，其特征在于：使用上述可变密钥的加密和解密利用硬件进行。

5. 权利要求 1 或权利要求 2 的数字数据保护方法，其特征在于：

上述可变密钥从使用装置外部供给.

6. 权利要求 1 或权利要求 2 的数字数据保护方法，其特征在于：上述可变密钥在使用装置内部生成.

7. 权利要求 1 或权利要求 2 的数字数据保护方法，其特征在于：使用上述固定密钥的加密和解密利用软件进行.

8. 权利要求 1 或权利要求 2 的数字数据保护方法，其特征在于：使用上述固定密钥的加密和解密利用硬件进行.

9. 权利要求 1 或权利要求 2 的数字数据保护方法，其特征在于：上述固定密钥一开始就内藏在上述使用装置中.

10. 权利要求 1 的数字数据保护方法，其特征在于：上述固定密钥在使用装置内部生成.

11. 权利要求 1 或权利要求 2 的数字数据保护方法，其特征在于：上述固定密钥从上述使用装置的外部供给.

12. 权利要求 9、权利要求 10 或权利要求 11 的数字数据保护方法，其特征在于：上述固定密钥是上述使用装置固有的.

13. 权利要求 9、权利要求 10 或权利要求 11 的数字数据保护方法，其特征在于：上述固定密钥不是上述使用装置固有的.

14. 一种对已将加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护装置，其特征在于：上述数字数据保护装置具有：

使用可变密钥对上述解密数字数据进行加密并将其作为再加密数字数据的可变密钥再加密单元；

为了保存、复制或转送上述可变密钥再加密数字数据利用使用装置内藏的固定密钥进行再加密并将其作为可变密钥一固定密钥双重再加密数字数据的固定密钥加密单元；

使用上述固定密钥对保存、复制或转送的上述可变密钥一固定密钥双重再加密数字数据进行解密并将其作为固定密钥再加密数字数据的固定密钥解密单元；

使用上述可变密钥对上述固定密钥再加密数字数据进行解密并将其作为上述解密数字数据的可变密钥解密单元.

15. 一种对已将加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护装置，其特征在于：上述数字数据保护装

置具有:

利用使用装置内藏的固定密钥对上述解密数字数据进行再加密并将其作为固定密钥再加密数字数据的固定密钥加密单元;

为了保存、复制或转送上述固定密钥再加密数字数据使用可变密钥进行加密并将其作为可变密钥一固定密钥双重再加密数字数据的可变密钥加密单元;

使用上述可变密钥对保存、复制或转送的上述可变密钥一固定密钥双重再加密数字数据进行解密并将其作为固定密钥再加密数字数据的可变密钥解密单元;

使用上述固定密钥对上述固定密钥再加密数字数据进行解密并将其作为上述解密数字数据的固定密钥解密单元.

16. 权利要求 14 或权利要求 15 的数字数据保护装置,其特征在于:使用上述可变密钥的加密和解密利用软件进行.

17. 权利要求 14 或权利要求 15 的数字数据保护装置,其特征在于:使用上述可变密钥的加密和解密利用硬件进行.

18. 权利要求 14 或权利要求 15 的数字数据保护装置,其特征在于:上述可变密钥从使用装置外部供给.

19. 权利要求 14 权利要求 15 的数字数据保护装置,其特征在于:上述可变密钥在使用装置内部生成.

20. 权利要求 14 或权利要求 15 的数字数据保护装置,其特征在于:使用上述固定密钥的加密和解密利用软件进行.

21. 权利要求 14 或权利要求 15 的数字数据保护装置,其特征在于:使用上述固定密钥的加密和解密利用硬件进行.

22. 权利要求 14 或权利要求 15 的数字数据保护装置,其特征在于:上述固定密钥一开始就内藏在上述使用装置中.

23. 权利要求 14 或权利要求 15 的数字数据保护装置,其特征在于:上述固定密钥在上述使用装置内部生成.

24. 权利要求 14 或权利要求 15 的数字数据保护装置,其特征在于:上述固定密钥从上述使用装置的外部供给.

25. 权利要求 22、权利要求 23 或权利要求 24 的数字数据保护装置,其特征在于:上述固定密钥是上述使用装置固有的.

26. 权利要求 22、权利要求 23 或权利要求 24 的数字数据保护装

置，其特征在于：上述固定密钥不是上述使用装置固有的。

27. 一种对已将第 1 可变密钥加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护方法，其特征在于：上述数字数据保护方法具有：

使用第 2 可变密钥对上述解密数字数据进行加密并将其作为第 2 可变密钥再加密数字数据的过程；

为了保存上述第 2 可变密钥再加密数字数据利用使用装置内藏的固定密钥进行加密并将其作为固定密钥一第 2 可变密钥双重再加密数字数据的过程；

使用上述固定密钥对保存的上述固定密钥一第 2 可变密钥双重再加密数字数据进行解密并将其作为上述第 2 可变密钥再加密数字数据的过程；

为了复制或转送上述第 2 可变密钥再加密数字数据使用第 3 可变密钥进行加密并将其作为第 3 可变密钥一第 2 可变密钥双重再加密数字数据的过程；

使用上述第 3 可变密钥对复制或转送的上述第 3 可变密钥一第 2 可变密钥双重再加密数字数据进行解密并将其作为第 2 可变密钥再加密数字数据的过程；

使用上述第 2 可变密钥对上述第 2 可变密钥再加密数字数据进行解密并将其作为解密数字数据的过程。

28. 一种对已将第 1 可变密钥加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护方法，其特征在于：上述数字数据保护方法具有：

使用第 2 可变密钥对上述解密数字数据进行加密并将其作为第 2 可变密钥再加密数字数据的过程；

为了保存上述第 2 可变密钥再加密数字数据利用使用装置内藏的固定密钥进行加密并将其作为固定密钥一第 2 可变密钥双重再加密数字数据的过程；

使用上述固定密钥对保存的上述固定密钥一第 2 可变密钥双重再加密数字数据进行解密并将其作为上述第 2 可变密钥再加密数字数据的过程；

为了复制或转送上述第 2 可变密钥再加密数字数据使用第 3 可变

密钥进行加密并将其作为第 3 可变密钥－第 2 可变密钥双重再加密数字数据的过程；

使用上述第 3 可变密钥对复制或转送的上述第 3 可变密钥－第 2 可变密钥双重再加密数字数据进行解密并将其作为第 2 可变密钥再加密数字数据的过程；

使用上述第 2 可变密钥对上述第 2 可变密钥再加密数字数据进行解密并将其作为解密数字数据的过程。

29. 一种对已将第 1 可变密钥加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护方法，其特征在于：上述数字数据保护方法具有：

为了保存上述解密数字数据利用使用装置内藏的固定密钥进行加密并将其作为固定密钥再加密数字数据、使用第 2 可变密钥对上述固定密钥再加密数字数据进行加密并将其作为第 2 可变密钥－固定密钥双重再加密数字数据的过程；

使用上述第 2 可变密钥对保存的上述第 2 可变密钥－固定密钥双重再加密数字数据进行解密并将其作为固定密钥再加密数字数据的过程；

使用上述固定密钥对上述固定密钥再加密数字数据进行解密并将其作为解密数字数据的过程；

为了复制或转送上述再加密数字数据使用第 3 可变密钥进行加密并将其作为第 3 可变密钥再加密数字数据、使用上述第 2 可变密钥对上述第 3 可变密钥再加密数字数据进行解密并将其作为第 2 可变密钥－第 3 可变密钥双重再加密数字数据的过程；

使用上述第 2 可变密钥对复制或转送的第 2 可变密钥－第 3 可变密钥双重再加密数字数据进行解密并将其作为第 3 可变密钥再加密数字数据的过程；

使用上述第 3 可变密钥对上述第 3 可变密钥再加密数字数据进行解密并将其作为解密数字数据的过程。

30. 一种对已将第 1 可变密钥加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护方法，其特征在于：上述数字数据保护方法具有：

为了保存上述解密数字数据利用使用装置内藏的固定密钥进行

加密并将其作为固定密钥再加密数字数据、使用第 2 可变密钥对上述固定密钥再加密数字数据进行加密并将其作为第 2 可变密钥—固定密钥双重再加密数字数据的过程;

使用上述第 2 可变密钥对保存的上述第 2 可变密钥—固定密钥双重再加密数字数据进行解密并将其作为固定密钥再加密数字数据的过程;

使用上述固定密钥对上述固定密钥再加密数字数据进行解密并将其作为解密数字数据的过程;

为了复制或转送上述再加密数字数据使用第 3 可变密钥进行加密并将其作为第 3 可变密钥再加密数字数据、使用上述第 2 可变密钥对上述第 3 可变密钥再加密数字数据进行解密并将其作为第 2 可变密钥—第 3 可变密钥双重再加密数字数据的过程;

使用上述第 2 可变密钥对复制或转送的第 2 可变密钥—第 3 可变密钥双重再加密数字数据进行解密并将其作为第 3 可变密钥再加密数字数据的过程;

使用上述第 3 可变密钥对上述第 3 可变密钥再加密数字数据进行解密并将其作为解密数字数据的过程.

31. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法,其特征在于:使用上述第 2 可变密钥的加密和解密利用软件进行.

32. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法,其特征在于:使用上述第 2 可变密钥的加密和解密利用硬件进行.

33. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法,其特征在于:上述第 2 可变密钥从外部供给.

34. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法,其特征在于:上述第 2 可变密钥在上述使用装置内部生成.

35. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法,其特征在于:使用上述第 3 可变密钥的加密和解密利用软件进行.

36. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的

数字数据保护方法，其特征在于：使用上述第 3 可变密钥的加密和解密利用硬件进行.

37. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法，其特征在于：上述第 3 可变密钥从使用装置的外部供给.

38. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法，其特征在于：上述第 3 可变密钥在上述使用装置内部生成.

39. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法，其特征在于：使用上述固定密钥的加密和解密利用软件进行.

40. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法，其特征在于：使用上述固定密钥的加密和解密利用硬件进行.

41. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法，其特征在于：上述固定密钥一开始就内藏在上述使用装置中.

42. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法，其特征在于：上述固定密钥在使用装置内部生成.

43. 权利要求 27、权利要求 28、权利要求 29 或权利要求 30 的数字数据保护方法，其特征在于：上述固定密钥从上述使用装置的外部供给.

44. 权利要求 41、权利要求 42 或权利要求 43 的数字数据保护方法，其特征在于：上述固定密钥是上述使用装置固有的.

45. 权利要求 41、权利要求 42 或权利要求 43 的数字数据保护方法，其特征在于：上述固定密钥不是上述使用装置固有的.

46. 一种对已将第 1 可变密钥加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护装置，其特征在于：上述数字数据保护装置具有：

使用第 2 可变密钥对上述解密数字数据进行加密并将其作为第 2 可变密钥再加密数字数据的第 2 可变密钥加密单元；

为了保存上述第 2 可变密钥再加密数字数据利用使用装置内藏的固定密钥进行加密并将其作为固定密钥一第 2 可变密钥双重再加密数字数据的固定密钥加密单元;

使用上述固定密钥对保存的上述固定密钥一第 2 可变密钥双重再加密数字数据进行解密并将其作为上述第 2 可变密钥再加密数字数据的固定密钥解密单元;

为了复制或转送上述第 2 可变密钥再加密数字数据使用第 3 可变密钥进行加密并将其作为第 3 可变密钥一第 2 可变密钥双重再加密数字数据的第 3 可变密钥加密单元;

使用上述第 3 可变密钥对复制或转送的上述第 3 可变密钥一第 2 可变密钥双重再加密数字数据进行解密并将其作为第 2 可变密钥再加密数字数据的第 3 可变密钥解密单元;

使用上述第 2 可变密钥对已解密的上述第 2 可变密钥再加密数字数据进行解密并将其作为解密数字数据的第 2 可变密钥解密单元.

47. 一种对已将第 1 可变密钥加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护装置, 其特征在于: 上述数字数据保护装置具有:

使用第 2 可变密钥对上述解密数字数据进行加密并将其作为第 2 可变密钥再加密数字数据的第 2 可变密钥加密单元;

为了保存上述第 2 可变密钥再加密数字数据利用使用装置内藏的固定密钥进行加密并将其作为固定密钥一第 2 可变密钥双重再加密数字数据的固定密钥加密单元;

使用上述固定密钥对保存的上述固定密钥一第 2 可变密钥双重再加密数字数据进行解密并将其作为上述第 2 可变密钥再加密数字数据的固定密钥解密单元;

为了复制或转送上述第 2 可变密钥再加密数字数据使用第 3 可变密钥进行加密并将其作为第 3 可变密钥一第 2 可变密钥双重再加密数字数据的第 3 可变密钥加密单元;

使用上述第 3 可变密钥对复制或转送的上述第 3 可变密钥一第 2 可变密钥双重再加密数字数据进行解密并将其作为第 2 可变密钥再加密数字数据的第 3 可变密钥解密单元;

使用上述第 2 可变密钥对已解密的上述第 2 可变密钥再加密数字

数据进行解密并将其作为解密数字数据的第 2 可变密钥解密单元.

48. 一种对已将第 1 可变密钥加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护装置，其特征在于：上述数字数据保护装置具有：

为了保存上述解密数字数据利用使用装置内藏的固定密钥进行加密并将其作为固定密钥再加密数字数据的固定密钥加密单元和使用第 2 可变密钥对上述固定密钥再加密数字数据进行加密并将其作为第 2 可变密钥一固定密钥双重再加密数字数据的第 2 可变密钥加密单元；

使用上述第 2 可变密钥对保存的上述第 2 可变密钥一固定密钥双重再加密数字数据进行解密并将其作为固定密钥再加密数字数据的第 2 可变密钥解密单元和使用上述固定密钥对上述固定密钥再加密数字数据进行解密并将其作为解密数字数据的固定密钥解密单元；

为了复制或转送上述再加密数字数据使用第 3 可变密钥进行加密并将其作为第 3 可变密钥再加密数字数据的第 3 可变密钥加密单元和使用上述第 2 可变密钥对上述第 3 可变密钥再加密数字数据进行解密并将其作为第 2 可变密钥一第 3 可变密钥双重再加密数字数据的第 2 可变密钥加密单元；

使用上述第 2 可变密钥对复制或转送的第 2 可变密钥一第 3 可变密钥双重再加密数字数据进行解密并将其作为第 3 可变密钥再加密数字数据的第 2 可变密钥解密单元和使用上述第 3 可变密钥对上述第 3 可变密钥再加密数字数据进行解密并将其作为解密数字数据的第 3 可变密钥解密单元.

49. 一种对已将第 1 可变密钥加密数字数据解密的解密数字数据进行保护防止其非法利用的数字数据保护装置，其特征在于：上述数字数据保护装置具有：

为了保存上述解密数字数据利用使用装置内藏的固定密钥进行加密并将其作为固定密钥再加密数字数据的固定密钥加密单元和使用第 2 可变密钥对上述固定密钥再加密数字数据进行加密并将其作为第 2 可变密钥一固定密钥双重再加密数字数据的第 2 可变密钥加密单元；

使用上述第 2 可变密钥对保存的上述第 2 可变密钥一固定密钥双

重再加密数字数据进行解密并将其作为固定密钥再加密数字数据的第2可变密钥解密单元和使用上述固定密钥对上述固定密钥再加密数字数据进行解密并将其作为解密数字数据的固定密钥解密单元；

为了复制或转送上述再加密数字数据使用第3可变密钥进行加密并将其作为第3可变密钥再加密数字数据的第3可变密钥加密单元和使用上述第2可变密钥对上述第3可变密钥再加密数字数据进行解密并将其作为第2可变密钥一第3可变密钥双重再加密数字数据的第2可变密钥加密单元；

使用上述第2可变密钥对复制或转送的第2可变密钥一第3可变密钥双重再加密数字数据进行解密并将其作为第3可变密钥再加密数字数据的第2可变密钥解密单元和使用上述第3可变密钥对上述第3可变密钥再加密数字数据进行解密并将其作为解密数字数据的第3可变密钥解密单元.

50. 权利要求46、权利要求47、权利要求48或权利要求49的数字数据保护装置，其特征在于：使用上述第2可变密钥的加密和解密利用软件进行.

51. 权利要求46、权利要求47、权利要求48或权利要求49的数字数据保护装置，其特征在于：使用上述第2可变密钥的加密和解密利用硬件进行.

52. 权利要求46、权利要求47、权利要求48或权利要求49的数字数据保护装置，其特征在于：上述第2可变密钥从使用装置的外部供给.

53. 权利要求46、权利要求47、权利要求48或权利要求49的数字数据保护装置，其特征在于：上述第2可变密钥在上述使用装置内部生成.

54. 权利要求46、权利要求47、权利要求48或权利要求49的数字数据保护装置，其特征在于：使用上述第3可变密钥的加密和解密利用软件进行.

55. 权利要求46、权利要求47、权利要求48或权利要求49的数字数据保护装置，其特征在于：使用上述第3可变密钥的加密和解密利用硬件进行.

56. 权利要求46、权利要求47、权利要求48或权利要求49的

数字数据保护装置，其特征在于：上述第 3 可变密钥从使用装置的外部供给。

57. 权利要求 46、权利要求 47、权利要求 48 或权利要求 49 的数字数据保护装置，其特征在于：上述第 3 可变密钥在上述使用装置内部生成。

58. 权利要求 46、权利要求 47、权利要求 48 或权利要求 49 的数字数据保护装置，其特征在于：使用上述固定密钥的加密和解密利用软件进行。

59. 权利要求 46、权利要求 47、权利要求 48 或权利要求 49 的数字数据保护装置，其特征在于：使用上述固定密钥的加密和解密利用硬件进行。

60. 权利要求 46、权利要求 47、权利要求 48 或权利要求 49 的数字数据保护装置，其特征在于：上述固定密钥一开始就内藏在上述使用装置中。

61. 权利要求 46、权利要求 47、权利要求 48 或权利要求 49 的数字数据保护装置，其特征在于：上述固定密钥在使用装置内部生成。

62. 权利要求 46、权利要求 47、权利要求 48 或权利要求 49 的数字数据保护装置，其特征在于：上述固定密钥从上述使用装置的外部供给。

63. 权利要求 60、权利要求 61 或权利要求 62 的数字数据保护装置，其特征在于：上述固定密钥是上述使用装置固有的。

64. 权利要求 60、权利要求 61 或权利要求 62 的数字数据保护装置，其特征在于：上述固定密钥不是上述使用装置固有的。

65. 一种保护数字数据防止其非法利用的数字数据保护方法，其特征在于：上述数字数据保护方法具有：

判定上述数字数据是否保护对象的过程；

使用内藏于上述使用装置的固定密钥对已判定是保护对象的上述数字数据进行加密并将其作为固定密钥加密数字数据的过程；

保存、复制或转送已判定不是保护对象的上述数字数据和上述固定密钥加密数字数据的过程；

使用上述固定密钥对保存、复制或转送的上述固定密钥加密数字

数据进行解密并将其作为解密数字数据的过程;

利用已保存、复制或转送的上述数字数据和上述解密数字数据的过程.

66. 权利要求 65 的数字数据保护方法，其特征在于：使用上述固定密钥的加密和解密利用软件进行.

67. 权利要求 65 的数字数据保护方法，其特征在于：使用上述固定密钥的加密和解密利用硬件进行.

68. 权利要求 65 的数字数据保护方法，其特征在于：使用上述固定密钥的加密和解密利用附加在上述数字数据中的识别符号来控制;

69. 权利要求 68 的数字数据保护方法，其特征在于：加密和解密利用具有上述识别符号来进行;

70. 权利要求 68 的数字数据保护方法，其特征在于：加密和解密利用没有上述识别符号来进行;

71. 权利要求 65 的数字数据保护方法，其特征在于：上述固定密钥一开始就内藏在使用装置中.

72. 权利要求 65 的数字数据保护方法，其特征在于：上述固定密钥在使用装置内部生成.

73. 权利要求 65 的数字数据保护方法，其特征在于：上述固定密钥从上述使用装置的外部供给.

74. 权利要求 71、权利要求 72 或权利要求和 73 的数字数据保护方法，其特征在于：上述固定密钥是上述使用装置固有的.

75. 权利要求 71、权利要求 72 或权利要求和 73 的数字数据保护方法，其特征在于：上述固定密钥不是上述使用装置固有的.

76. 一种保护数字数据防止其非法利用的数字数据保护装置，其特征在于：上述数字数据保护装置具有:

判定上述数字数据是否保护对象的过程;

使用内藏于上述使用装置的固定密钥对已判定是保护对象的上述数字数据进行加密并将其作为固定密钥加密数字数据的过程;

保存、复制或转送已判定不是保护对象的上述数字数据和上述固定密钥加密数字数据的过程;

使用上述固定密钥对保存、复制或转送的上述固定密钥加密数字

数据进行解密并将其作为解密数字数据的过程;

利用已保存、复制或转送的上述数字数据和上述解密数字数据的过程.

77. 权利要求 76 的数字数据保护装置，其特征在于：使用上述固定密钥的加密和解密利用软件进行.

78. 权利要求 76 的数字数据保护装置，其特征在于：使用上述固定密钥的加密和解密利用硬件进行.

79. 权利要求 76 的数字数据保护装置，其特征在于：使用上述固定密钥的加密和解密利用附加在上述数字数据中的识别符号来控制;

80. 权利要求 76 的数字数据保护装置，其特征在于：加密和解密利用具有上述识别符号来进行;

81. 权利要求 76 的数字数据保护装置，其特征在于：加密和解密利用没有上述识别符号来进行;

82. 权利要求 76 的数字数据保护装置，其特征在于：上述固定密钥一开始就内藏在使用装置中.

83. 权利要求 76 的数字数据保护装置，其特征在于：上述固定密钥在使用装置内部生成.

84. 权利要求 76 的数字数据保护装置，其特征在于：上述固定密钥从上述使用装置的外部供给.

85. 权利要求 82、权利要求 83 或权利要求和 84 的数字数据保护装置，其特征在于：上述固定密钥是上述使用装置固有的.

86. 权利要求 82、权利要求 83 或权利要求和 84 的数字数据保护装置，其特征在于：上述固定密钥不是上述使用装置固有的.

说　明　书

利用双重加密保护数字数据的方法及装置

技术领域

本发明涉及通过对数字音像资料（contents）进行管理、特别对拥有著作权的数字音像资料进行著作权管理以及对数字音像资料进行保密来实现数字音像资料的流通和数字音像资料经济的方法及装置.

背景技术

过去广泛普及的模拟音像资料每当进行保存、复制、加工和转送时，其质量都会下降，所以，因这样一些工作而带来的著作权的处理不是很大的问题. 但是，数字音像资料因即使反复进行保存、复制、加工和转送其质量也不会降低，所以，因这样一些工作而带来的著作权的处理就是很大的问题.

数字图像、声音等数字数据大多通过播送、DVD 等以收费方式向用户提供，这时，为了防止不交费视听，对其加密后再向用户提供. 加密后提供的数字数据使用以某种手段提供的密码密钥对其解密后再进行视听. 因解密后的数字数据即使通过保存、复制或转送其质量也不会降低，故当用户进行保存、复制或转送时，可以进行 2 次不缴费视听，为了保护音像资料提供者的利益，防止已解密的数字音像资料的再次被利用，开发了一些用来禁止再次利用、即保存、复制或转送等 2 次利用的系统和设备.

但是，禁止 2 次利用对使用者来说，数字音像资料就缺乏吸引力，很可能成为阻碍数字音像资料普及的主要原因. 因为认识到了这一点，所以提出一种方案，通过对已解密的数字音像资料进行再加密，可以防止非法使用，同时，又能够吸引使用者来使用数字音像资料.

对于将数字数据存储在媒体中再转让或租借给用户以及已转送给用户的数字数据的保存、复制或转送等的 2 次利用，因数字数据已在用户手中，所以，数字数据的著作权所有者本身不可能对其进行著作权保护，有必要使用某种方法自动地强制地进行.

鉴于这种情况，迄今为止，本发明者以保护数字音像资料的著作权为目的已提出了多种方案.

本发明者在特开平 6－46419 号（GB2269302，USSN08/098415）和特开平 6－141004 号（USP5794115，USP5901339）号公报中公开了通过公共电话线从密钥管理中心得到允许密钥来进行著作权管理的系统，并在特开平 6－132916 号（GB2272822，USSN08/135634）公报中公开了实现该系统的装置.

此外，在特开平 7－271865 号（EP0677949A2，USSN08/416037）和特开平 8－185448 号（EP0704785A2，USSN08/536747）公报中又公开了管理数字音像资料的著作权的系统.

在这些系统及装置中，希望收看已加密的节目的人使用通信装置并经由通信线路向管理中心提出视听申请，管理中心对该视听申请发送许可密钥，同时进行收费处理并征收费用.

已接收许可密钥的视听申请者利用在线或离线装置将许可密钥送入接收装置，已送入许可密钥的接收装置利用该许可密钥对已加密的节目进行解密.

特开平 7－271865 号（EP0677949A2，USSN08/416037）公报记载的系统为了进行包含数字音像资料的实时发送的数据库系统中的数字音像资料的显示（包含发声）、保存、复制、加工和转送时的著作权管理，除了利用许可密钥之外，还使用用来管理著作权的程序和著作权信息.

该著作权管理程序进行监视和管理，以便防止非法使用与申请和许可的内容相违背的资料.

此外，该特开平 7－271865 号（EP0677949A2，USSN08/416037）公报记载了从数据库提供加密状态的数字音像资料，并利用著作权管理程序，只在显示和加工时才进行解密，而保存、复制和转送则在再加密的状态下进行. 进而还记载了对著作权管理程序本身进行加密，并利用许可密钥对著作权管理程序进行解密，已解密的著作权管理程序进行著作权数据的解密和加密，同时，当进行数据的保存和显示以外的使用时，将包含操作者信息的著作权信息附加在原著作权信息之上并作为历史资料保存下来.

特开平 8－287014 号（USP5867579，EP0715241A2）公报提出了用来进行著作权管理的接口、PCMCIA 卡或 IC 卡，一种具有 IC 形态的解密/再加密装置和密码密钥的寄存系统. 此外，该专利还提及了著

作权管理方法在电视会议和电子商务系统中的应用.

再有，USP5805706 也记载了具有 IC 形态的解密/再加密装置.

特开平 8—272745 号（USP5646999，EP0709760）公报提出了一种系统，通过将秘密密钥（公共密钥）方式和公开密钥方式结合起来对加工程序进行数字署名来确认申请的合法性，由此进行利用了多个数据来加工数据的原数据著作权和加工数据著作权的保护.

特开平 8—288940 号（USP5740246，EP0719045A2）公报提出了各种适用于数据库、电视点播（VOD: Vedio-on-demand）系统或电子商务中的著作权管理系统的形态.

特开平 8—329011 号（USP5848158，EP0746126A2）公报提出了使用第 3 密码密钥和著作权标记进行使用或加工多个数据时的原数据和新数据的著作权保护的系统.

由以上说明的本发明提出的数据著作权管理系统和数据著作权管理装置可知，数据著作权管理可以通过利用著作权管理程序进行加密/解密/再加密和对使用内容进行限制来实现. 该加密技术和使用限制可以通过使用计算机来实现.

进而，在经由网络交换信息时，为了防止窃取而进行信息的加密.

在 USP5504818、5515441 中叙述了利用加密来防止传送时窃取信息的方法，这时，在 USP5504816、5353351、5475757 和 5381480 中叙述了使用多个密钥的方法，在 USP5479514 中叙述了进行再加密的方法.

利用著作权管理程序进行数字数据的二次利用的著作权保护可以通过对已解密的数字数据进行再加密/再解密以及通过利用著作权管理程序去管理并执行该再加密/再解密来实现.

当然，作为进行再加密/再解密的方法有使用软件的方法和使用硬件的方法.

使用密钥 K 从非加密数据 M 得到加密数据 C 可以由

$$C = E(M, k)$$

表示，使用密钥 K 从加密数据 C 得到解密数据 M 可以由

$$M = D(C, k)$$

表示.

此外，反复进行解密数据 M 的再加密/再解密时的再解密可以由

Ai: Ci = E(D(Ci-1, Ki-1), Ki)　　I 是正整数

表示，再解密可以由

∃: M = D(E(Ci-1, Ki-1), Ki)

表示。

根据图 1 说明过去提案的机顶盒（STB）的构成及用该机顶盒进行的数字数据的保护方法。

再有，在该说明中，省略了与加密/解密无直接关系的外围电路、例如放大单元和压缩/解压缩单元。

在该图中，1 是由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据，为了防止非法使用，使用第 1 可变密钥 K1 进行加密，

C1 = E(M, K1)

并供给机顶盒 2.

在已供给加密数字数据 C1 的机顶盒 2 中，使用通过和加密数字数据 C1 相同的路径或和加密数字数据 C1 不同的路径从密钥中心得到的第 1 可变密钥 K1，在解密单元 3 中对加密数字数据 C1 进行解密，

M = D(C1, K1)

得到的解密数据 M 向显示装置 4 等输出.

当解密数据 M 保存在数字视盘 RAM(DVD)或硬盘等媒体中或经由网络向外部传送时，在固定方式加密/解密单元 5 的加密单元 6 中，使用固定密钥 K0 对解密数据 M 进行再加密，

A0: C0 = E(M, K0)

= E(D(C1, K1), K0)

并作为再加密数据 C0 保存在外部装置 8 中或进行转送.

当再利用再加密数据 C0 时，在固定方式加密/解密单元 5 的解密单元 7 中，对从外部装置 8 的保存媒体中读出或经由网络转送来的再加密数据 C0，使用固定密钥 K0 进行再解密，

∃: M = D(C0, K0)

= D(E(D(C1, K1), K0)

解密数据 M 输出给显示装置 4 等.

这时，为了保证安全，也可以构成为：当经由图中虚线所示路径

从保存媒体中读出再加密数据 C0 时，保存媒体中的再加密数据 C0 被删去，再使用固定密钥 K0 再保存再加密了的数据.

再有，在美国专利 5805706 号中，示出了进行再加密/再解密的集成电路.

这样构成的机顶盒因利用硬件并使用固定密钥 K0 自动进行再加密/再解密，故容易进行处理，而且对必需保护的数字数据强制性地进行再加密/再解密是有效的.

但是，当固定密钥 K0 装在装置内时，密码密钥 K0 恐怕会被破译，在这种情况下，以后对该数字数据就不可能进行保护.

发明概要

为了解决该问题，本申请提供的发明是在使用固定密钥再加密的基础上使用可变密钥进行双重再加密的方法及装置.

按固定密钥和可变密钥的使用顺序来分，有开始使用可变密钥其次使用固定密钥的情况和开始使用固定密钥其次使用可变密钥的情况.

因最开始用于再加密的密钥在最后解密时使用，故即使在后面进行的再加密被破译的情况下，破译的难度也相当大. 因此，当开始使用可变密钥其次使用固定密钥进行再加密时，即使知道固定密钥，知道可变密钥的可能性也很小.

作为实施形态有利用软件和利用硬件的情况，进而还有软硬件组合的情况. 作为硬件，可以利用面向数字图像开发的使用固定密钥的硬件.

为了保证利用软件时的程序和使用的密钥的安全性，在用户不能利用的核心部以下的区域进行加密/解密. 具体地说，在 I/O 管理程序内的设备驱动程序、即滤波驱动程序、盘驱动/网络驱动程序和利用 HAL 的实时 OS 中进行加密/解密. 滤波驱动程序有 2 个，将文件系统驱动程序夹在中间，利用哪一个都行，也可以 2 个都利用.

附图的简单说明

图 1 是过去提案的机顶盒的概要构成说明图.

图 2 是适用于机顶盒的第 1 实施例的概要构成的说明图.

图 3 是适用于机顶盒的第 2 实施例的概要构成说明图.

图 4 是适用于使用了个人计算机的装置的第 3 实施例的概要构成

说明图.

图 5 是适用于使用了个人计算机的装置的第 4 实施例的概要构成说明图.

图 6 是第 4 实施例的详细说明图.

图 7 是适用于使用了个人计算机的装置的第 5 实施例的概要构成说明图.

图 8 是作为第 1 实施例的变形例的第 6 实施例的机顶盒的概要构成说明图.

图 9 是作为第 6 实施例的变形例的第 7 实施例的机顶盒的概要构成说明图.

图 10 是使用了个人计算机的第 8 实施例的概要构成说明图.

图 11 是第 8 实施例的详细说明图.

图 12 是著作权管理装置的实施例说明图.

图 13 是著作权管理装置的另一实施例说明图.

图 14 是著作权管理装置的又一实施例说明图.

实施本发明的最佳形态

说明本发明的实施例.

根据图 2 说明适用于本发明的第 1 实施例的机顶盒（STB）的构成和用该机顶盒进行的数字数据保护方法.

再有，该实施例的机顶盒也和图 1 所示的先有例的机顶盒的情况一样，省略了与加密/解密无直接关系的外围电路、例如放大单元、压缩/解压缩单元及向外部装置的接口装置的说明.

该实施例与图 1 所示的过去提案的机顶盒不同之点在于：在解密单元 13 和使用固定密钥 KO 进行加密/解密的固定密钥方式加密/解密单元 15 之间插入使用第 2 可变密钥 K2 进行加密/解密的可变密钥方式加密/解密单元 19. 该第 2 可变密钥 K2 有从外部供给的情况和在机顶盒内生成的情况.

在该图中，11 是由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据，为了防止非法使用，使用第 1 可变密钥 K1 进行加密，

$$C1 = E(M, K1)$$

并供给机顶盒 12.

在已供给加密数字数据 C1 的机顶盒 12 中，使用通过和加密数字数据 C1 相同的路径或和加密数字数据 C1 不同的路径从密钥中心得到的第 1 可变密钥 K1，在解密单元 13 中对加密数字数据 C1 进行解密，

M = D（C1，K1）

得到的解密数据 M 向显示装置 14 等输出。

当拥有著作权的解密数据 M 保存在数字视盘（DVD）RAM 或硬盘等媒体的外部装置 18 中或经由网络向外部传送时，在可变密钥方式加密/解密单元 19 的加密单元 20 中，使用第 2 可变密钥 K2 对解密数据 M 进行再加密，

A2: C2 = E（M，K2）

= E（D（C1，K1），K2）

进而，在固定密钥方式加密/解密单元 15 的加密单元 16 中，使用固定密钥 K0 对再加密数据 C2 进行再再加密，

A2-0: C2-0 = E（C2，K0）

= E（E（D（C1，K1），K2），K0）

并作为再再加密数据 C2-0 保存在外部装置 18 中或进行转送。

当再利用再再加密数据 C2-0 时，在内藏的固定方式加密/解密单元 15 的解密单元 17 中，对从外部装置 18 的保存媒体中读出或经由网络转送来的再加密数据 C2-0，使用固定密钥 K0 进行再解密，

∃2: C2 = E（C2-0，K0）

= D（E（E（D（C1，K1），K2），K0）

进而，在可变密钥方式加密/解密单元 19 的解密单元 21 中，对再解密数据 C2，使用可变密钥 K2 进行解密，

∃: M = D（C2，K2）

= D（E（D（C1，K1），K2）

得到的解密数据 M 输出给显示装置 14 等。

这时，为了保证安全，也可以构成为：当经由图中虚线所示路径从保存媒体中读出再加密数据 C2-0 时，保存媒体中的再加密数据 C2-0 被删去，再使用可变密钥 K2 和固定密钥 K0 再保存已再加密了的数据。

这样，在使用固定密钥 K0 再加密之前使用第 2 可变密钥 K2 进行再加密，利用这样的结构，即使万一固定密钥 K0 被破译，因数据还

可以通过第 2 可变密钥 K2 加密，所以，进一步破译第 2 可变密钥 K2 来进行加密数据的解密就变得十分困难.

此外，第 2 可变密钥 K2 最初用于再加密，而在使用固定密钥 K0 进行了再再加密和再解密之后，再用于再再解密，所以，第 2 可变密钥 K2 的安全性高，而且，因最初被使用故能强有力地支配加密数据.

在该实施例中，就加密单元 20 和解密单元 21 包含在可变密钥加密/解密单元 19 中、加密单元 16 和加密单元 17 包含在固定密钥加密/解密单元 15 中的情况进行了说明，当然也可以将这些单元 16、17、20、21 分开设置.

再有，这样的动作通过在机顶盒 12 内设置具有 CPU 和系统总线的计算机结构就能够容易实现.

根据图 3 说明适用于本发明的第 2 实施例的机顶盒（STB）的另一构成和用该机顶盒进行的数字数据保护方法.

再有，该第 2 实施例的机顶盒也和图 1 所示的先有例的机顶盒的情况一样，省略了与加密/解密无直接关系的外围电路、例如放大单元、压缩/解压缩单元的说明.

该第 2 实施例的机顶盒与图 2 所示的第 1 实施例的机顶盒不同之点在于：使用固定密钥 K0 进行加密/解密的固定密钥方式加密/解密单元 35 和使用第 2 可变密钥 K2 进行加密/解密的可变密钥方式加密/解密单元 39 的插入位置互相置换.

即，使用固定密钥 K0 进行加密/解密的固定密钥方式加密/解密单元 35 与解密单元 33 和显示器 34 连接，外部装置 38 与使用第 2 可变密钥 K2 进行加密/解密的可变密钥方式加密/解密单元 39 连接. 该第 2 可变密钥 K2 有从外部供给的情况和在机顶盒内生成的情况.

在该图中，31 是由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据，为了防止非法使用，使用第 1 可变密钥 K1 进行加密，

$$C1 = E(M, K1)$$

并供给机顶盒 32.

在已供给加密数字数据 C1 的机顶盒 32 中，使用通过和加密数字数据 C1 相同的路径或和加密数字数据 C1 不同的路径从密钥中心得到的第 1 可变密钥 K1，在解密单元 33 中对加密数字数据 C1 进行解密，

M = D（C1，K1）

得到的解密数据M向显示装置34等输出。

当拥有著作权的解密数据M保存在数字视盘（DVD）RAM或硬盘等媒体的外部装置38中或经由网络向外部传送时，在固定密钥方式加密/解密单元35的加密单元36中，使用固定密钥K0对再加密数据C2进行再加密，

A0: C0 = E（M，K0）

= E（D（C1，K1），K0）

进而，在可变密钥方式加密/解密单元39的加密单元40中，使用第2可变密钥K2对解密数据M进行再再加密，

A0-2: C0-2 = E（C0，K2）

= E（E（D（C1，K1），K0），K2）

并作为再再加密数据C0-2保存在外部装置38中或进行转送。

当再利用再再加密数据C0-2时，在可变密钥方式加密/解密单元39的解密单元41中，对从外部装置38的保存媒体中读出或经由网络转送来的再加密数据C0-2，使用第2可变密钥K2进行再解密，

ヨ0: C0 = E（C0-2，K2）

= D（E（E（D（C1，K1），K0），K2）

进而，在固定密钥方式加密/解密单元35的解密单元37中，对再解密数据C0，使用固定密钥K0进行再再解密，

ヨ: M = D（C0，K0）

= D（E（D（C1，K1），K0）

得到的解密数据M输出给显示装置34等。

这时，为了保证安全，也可以构成为：当经由图中虚线所示路径从保存媒体中读出再加密数据C0-2时，保存媒体中的再再加密数据C0-2被删去，使用固定密钥K0和第2可变密钥K2再保存已再加密了的数据。

这样，在使用固定密钥K0再加密之前使用第2可变密钥K2进行再加密，利用这样的结构，假如固定密钥K0被破译，因数据还可以通过第2可变密钥K2加密，所以，进一步破译第2可变密钥K2来进行加密数据的解密就变得十分困难。

此外，因该结构只是在图1所示的过去提案的机顶盒的固定密钥

方式加密/解密单元 35 的基础上单纯地附加了可变密钥方式加密/解密单元 39，所以，机顶盒的设计较容易。

在该实施例中，就加密单元 36 和解密单元 37 包含在固定密钥加密/解密单元 35 中、加密单元 40 和加密单元 41 包含在可变密钥加密/解密单元 39 中的情况进行了说明，当然也可以将这些单元 36、37、40、41 分开设置。

再有，这样的动作通过在机顶盒 32 内设置具有 CPU 和系统总线的计算机结构就能够容易实现。

数字音像资料的处理不仅可以通过机顶盒来进行也可以通过个人计算机等计算机来进行。

根据图 4 到图 7 说明适用于使用了个人计算机的装置的本发明的实施例。

个人计算机与象机顶盒那样完全由硬件构成只由硬件工作的装置不同，是使用软件去控制装在装置内的硬件来使其工作的装置。

为了有效地使用计算机，使用操作系统（OS）来控制计算机的整个动作。

以往个人计算机等使用的操作系统由进行存储器管理、任务管理、中断、过程间通信的基本服务的核心（Kernel）和进行其它服务的操作系统服务构成。

但是，伴随微处理器能力的提高和作为主存储装置使用的 RAM 的价格的降低的计算机方面形势的变化以及使用者对计算机性能的要求的提高，对控制整个计算机的动作的操作系统的功能的要求也提高来，与以前相比，操作系统的规模变得很庞大。

这样庞大的操作系统其本身要占用很大的硬盘空间来保存该操作系统，所以，保存用户必要的应用程序或数据的空间往往不足，会发生计算机使用不顺手的情况。

为了应付这样的的情况，最新的操作系统将进行其它操作系统的模拟和绘图的环境子系统以及安全子系统等中枢子系统作为依赖于用户的部分的子系统从核心中除去，将吸收硬件之间的差异的 HAL（硬件吸收层：Hardware abstraction Layer）、调度功能、中断功能、I/O 管理功能等基本部分作为微核心（Micro kernel），并在子系统和微核心之间插入系统服务 API（应用程序设计界面），这样来构成

操作系统.

这样一来，通过改变或追加功能来提高操作系统的扩展性能，容易实现与用途对应的移植.

此外，通过将微核心的要素分散配置在已网络化的多个计算机中，容易实现分散操作系统.

计算机除以台式或笔记本型为代表的个人计算机之外，可以用于计算机外围设备、各种控制装置和通信机等. 这时，作为适用于各种装置的嵌入用的专用操作系统，与注重人机接口的通用个人计算机用的操作系统不同，采用注重快速执行的实时操作系统.

装入每一个装置的专用操作系统都不同，当然专用开发操作系统的开发费用大. 因此，最近，提出转用个人计算机用的通用操作系统来作为嵌入用的实时操作系统，通过将嵌入用的固有程序配置在与微核心组合的子系统中来得到嵌入用的实时操作系统.

作为操作系统的一个很大的功能，有调度和中断处理等的任务管理.

在操作系统中任务管理大致有两种方式，即在同一时间只进行 1 个任务处理的单任务方式和同时进行多个任务的多任务方式，多任务方式进而又分为任务转换依赖于所处理的任务的多任务方式和不依赖与所处理的任务的多任务方式.

在它们中间，单任务方式是将 1 个过程分配给 MPU 在该任务结束之前不释放 MPU 的方式，非占先式多任务方式虽然可以对 MPU 进行时分割再分配给多个过程，但只要执行中的过程不使控制返回操作系统就不执行其它的过程，占先式多任务方式以某一时间间隔对执行中的过程进行中断，强制性地使控制转移到其它过程中.

因此，实时的多任务只有在占先方式的情况下才有可能.

计算机中的任务管理按过程进行，过程是具有存储器和文件等系统资源的单位，过程的管理按线程进行，线程是将过程细分后的分配 CPU 时间的单位. 再有，这时，系统资源由同一过程内的所有的线程所共有，因此，在一个过程中存在一个以上共有系统资源的线程.

用多任务方式处理的各任务有优先顺序（Priority Spectrum），一般，分为 32 级. 这时，不进行中断的通常的任务是分成 0-15 级的动态类型（Dynamic Class），进行中断的任务是分成 16-31 级的实

时类型（Real-Time Class）.

中断处理以被称作时间片的中断可能时间（通常 10ms）为单位进行，通常的中断以 10ms 的时间片进行.

在这样的的状况下，最近提出了被称作实时时间片的中断可能时间为 100μs 的时间片，但若利用该实时时间片，则有可能比过去的 10ms 中断优先中断.

在图 4 所示的第 3 实施例中，利用软件进行的可变密钥方式加密/解密处理和加密密钥的计算机管理在 HAL 中利用实时 OS 进行.

在该图中，51 是计算机内的操作系统，56 是显示计算机输出的显示装置，57 是固定密钥方式加密/解密单元，58 是数字视盘（DVD）RAM 或硬盘等数据保存媒体或网络等数据转送装置.

操作系统 51 由作为用户区的操作系统服务部 52、系统服务 API 部 53、作为非用户区的核心部 54 和 HAL55 构成，系统服务 API 部 53 配置在操作系统服务部 52 和核心部 54 之间，起调停操作系统服务部 52 和核心部 54 的作用. HAL55 配置在操作系统 50 的最下层，起吸收硬件和硬件之间的软件上的差异的作用.

操作系统服务部 52 由应用 59、子系统 60 和安全子系统构成，核心部 54 由多个微核心模块 62、64 和核心 63 构成，微核心模块 62 具有调度、中断等任务管理功能，微核心模块 64 具有 I/O 管理功能.

具有 I/O 管理功能的微核心模块 64 由 I/O 管理程序 65、由 I/O 管理程序管理的盘驱动程序 67 和网络驱动程序 68 等设备驱动程序、以及必要时插在 I/O 管理程序 65 和由 I/O 管理程序管理的盘驱动程序 67 及网络驱动程序 68 等设备驱动程序之间的滤波器驱动程序 66 构成.

计算机的可变密钥方式加密/解密处理利用软件进行，但在第 3 实施例的情况下，可变密钥方式加密/解密处理在操作系统 51 内的 HAL55 中优先其它任务，利用前面说明过的实时 OS（RTOS）进行.

与图 2 所示的第 1 实施例的情况一样，为了防止非法使用，由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据使用第 1 可变密钥 K1 进行加密，

C1 = E（M, K1）

并提供，已供给加密数字数据 C1 使用通过和加密数字数据 C1 相同的路径或和加密数字数据 C1 不同的路径从密钥中心提供的第 1 可变密钥 K1，利用操作系统服务部 52 进行解密，

M = D（C1，K1）

得到的解密数据 M 向显示装置 56 等输出。

当拥有著作权的解密数据 M 保存在数字视盘（DVD）RAM 或硬盘等媒体中或经由网络向外部传送时，在 HAL55 中，使用第 2 可变密钥 K2 对解密数据 M 强制进行再加密，

A2: C2 = E（M，K2）

= E（D（C1，K1），K2）

进而，在固定密钥方式加密/解密装置 57 中，使用固定密钥 KO 对再加密数据 C2 进行再再加密，

A2-O: C2-O = E（C2，KO）

= E（E（D（C1，K1），K2），KO）

并作为再再加密数据 C2-O 保存在外部装置 58 中或进行转送。该可变密钥 K2 有从外部供给的情况和在机顶盒内部生成的情况。

当利用再再加密数据 C2-O 时，在固定方式加密/解密装置 57 中，对从保存媒体读出或经由网络转送来的再加密数据 C2-O，使用固定密钥 KO 进行再解密，

∃ 2: C2 = E（C2-O，KO）

= D（E（E（D（C1，K1），K2），KO）

进而，在具有可变密钥方式加密/解密功能的 HAL55 中，对再解密数据 C2，使用第 2 可变密钥 K2 进行解密，

∃: M = D（C2，K2）

= D（E（D（C1，K1），K2）

得到的解密数据 M 输出给显示装置 56 等。

实时 OS 比其它所有的任务优先执行，在该第 3 实施例中，因实时 OS 在作为操作系统与硬件的接点的 HAL 中执行，所以，不可能可靠地进行数字数据的再加密，也不可能将解密数据 M 直接在外部装置 58 中保存或进行转送。此外，通过在使用固定密钥 KO 再加密之前使用第 2 可变密钥 K2 进行再加密，即使固定密钥 KO 被破译，因数据还可以通过第 2 可变密钥 K2 加密，所以，进一步破译第 2 可变密钥 K2

来进行加密数据的解密就变得十分困难.

此外，第 2 可变密钥 K2 最初用于再加密，而在使用固定密钥 K0 之后，又在最后被使用，所以，密钥的安全性高，而且，因最初被使用故能强有力地支配加密数据.

这样的动作通过使固定方式加密/解密装置 57 是具有 CPU 和系统总线的子计算机结构就能够容易实现.

在图 5 所示的第 4 实施例中，利用软件进行的可变密钥方式加密/解密处理和加密密钥的计算机处理在插在核心部 54 内的 I/O 管理微核心模块 64 中的滤波器驱动程序 66 中进行.

图 6 所示的结构是插入了滤波器驱动程序 66 的 I/O 管理微核心模块 64 的结构.

未插入滤波器驱动程序的 I/O 管理微核心模块从上位层到下位层配置有文件系统驱动程序 69、中间驱动程序 70 和设备驱动程序 71，必要时，在文件系统驱动程序 69 的上位层或中间驱动程序 70 和设备驱动程序 71 之间插入滤波器驱动程序 66A 或滤波器驱动程序 66B.

因可以在这些滤波器驱动程序 66A 和滤波器驱动程序 66B 中进行再加密/再解密处理和密钥的管理，故在该实施例中，再加密/再解密处理和密钥的管理在滤波器驱动程序 66A 或滤波器驱动程序 66B 中进行.

滤波器驱动程序不是配置在用户可操作的操作系统服务部 52，而是配置在用户不能操作的核心部 54. 但是，一般要根据使用操作系统的计算机来改变规更正规格参数，特别改变 I/O 管理模块的内容的情况也不少见.

利用这一特点，在第 4 实施例中，具有再加密/再解密处理和密钥的管理功能的模块作为滤波器驱动程序 66A 或滤波器驱动程序 66B 插入 I/O 管理模块中.

与图 2 所示的第 1 实施例的情况一样，为了防止非法使用，由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据使用第 1 可变密钥 K1 进行加密，

$$C1 = E(M, K1)$$

并提供，已供给加密数字数据 C1 使用通过和加密数字数据 C1 相同的

路径或和加密数字数据 C1 不同的路径从密钥中心提供的第 1 可变密钥 K1，利用操作系统服务部 52 进行解密，

M = D（C1，K1）

得到的解密数据 M 向显示装置 56 等输出.

当拥有著作权的解密数据 M 保存在数字视盘（DVD）RAM 或硬盘等媒体中或经由网络向外部传送时，在滤波器驱动程序 66A 和 66B 中，使用第 2 可变密钥 K2 对解密数据 M 强制进行再加密，

A2: C2 = E（M，K2）

= E（D（C1，K1），K2）

进而，在固定密钥方式加密/解密装置 57 中，使用固定密钥 KO 对再加密数据 C2 进行再再加密，

A2-O: C2-O = E（C2，KO）

= E（E（D（C1，K1），K2），KO）

并作为再再加密数据 C2-O 保存在外部装置 58 中或进行转送. 该可变密钥 K2 有从外部供给的情况和在机顶盒内部生成的情况.

当再利用再再加密数据 C2-O 时，在固定方式加密/解密装置 57 中，对从保存媒体读出或经由网络转送来的再加密数据 C2-O，使用固定密钥 KO 进行再解密，

彐 2: C2 = E（C2-O，KO）

= D（E（E（D（C1，K1），K2），KO）

进而，在滤波器驱动程序 66A 和 66B 中，对再解密数据 C2，使用第 2 可变密钥 K2 进行解密，

彐: M = D（C2，K2）

= D（E（D（C1，K1），K2）

得到的解密数据 M 输出给显示装置 56 等.

滤波器驱动程序作为 I/O 管理模块的一部分容易插入操作系统的核心部，这样一来，容易将加密/解密处理和密钥的管理功能装入操作系统. 此外，通过在使用固定密钥 KO 再加密之前使用第 2 可变密钥 K2 进行再加密，即使固定密钥 KO 被破译，因数据还可以通过第 2 可变密钥 K2 加密，所以，进一步破译第 2 可变密钥 K2 来进行加密数据的解密就变得十分困难.

此外，第 2 可变密钥 K2 最初用于再加密，而在使用固定密钥 KO

之后，又在最后被使用，所以，密钥的安全性高，而且，因最初被使用故能强有力地支配加密数据.

这样的动作通过使固定方式加密/解密装置 57 是具有 CPU 和系统总线的子计算机结构就能够容易实现.

在图 7 所示的第 5 实施例中，利用软件进行的可变密钥方式加密/解密处理和加密密钥的计算机管理在包含在操作系统 51 内的 I/O 管理微核心模块 64 中的盘驱动程序 57 和网络驱动程序 68 中进行.

如用图 6 说明的那样，I/O 管理微核心模块从上位层到下位层配置有文件系统驱动程序 69、中间驱动程序 70 和设备驱动程序 71，位于最下层的设备驱动程序 71 也可以进行可变密钥方式加密/解密处理和密钥管理.

与图 2 所示的第 1 实施例的情况一样，为了防止非法使用，由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据使用第 1 可变密钥 K1 进行加密，

$$C1 = E(M, K1)$$

并提供，已供给加密数字数据 C1 使用通过和加密数字数据 C1 相同的路径或和加密数字数据 C1 不同的路径从密钥中心提供的第 1 可变密钥 K1，利用操作系统服务部 52 进行解密，

$$M = D(C1, K1)$$

得到的解密数据 M 向显示装置 56 等输出.

当拥有著作权的解密数据 M 保存在数字视盘(DVD)RAM 或硬盘等媒体中或经由网络向外部传送时，在作为盘驱动程序 67 及网络驱动程序 68 的设备驱动程序 71 中，使用第 2 可变密钥 K2 对解密数据 M 强制进行再加密，

$$A2:\ C2 = E(M, K2)$$
$$= E(D(C1, K1), K2)$$

进而，在固定密钥方式加密/解密装置 57 中，使用内藏在固定密钥方式加密/解密装置 57 中的固定密钥 K0 对再加密数据 C2 进行再再加密，

$$A2\text{-}0:\ C2\text{-}0 = E(C2, K0)$$
$$= E(E(D(C1, K1), K2), K0)$$

并作为再再加密数据 C2-0 保存在外部装置 58 中或进行转送. 该可变密钥 K2 有从外部供给的情况和在机顶盒内部生成的情况.

当再利用再再加密数据 C2-0 时, 在内藏固定密钥方式加密/解密装置 57 中, 对从保存媒体读出或经由网络转送来的再加密数据 C2-0, 使用固定密钥 K0 进行再解密,

$$\exists\ 2:\ C2 = E(C2\text{-}0,\ K0)$$
$$= D(E(E(D(C1,\ K1),\ K2),\ K0)$$

进而, 在作为盘驱动程序 67 及网络驱动程序 68 的设备驱动程序 71 中, 对再解密数据 C2, 使用可变密钥 K2 进行解密,

$$\exists:\ M = D(C2,\ K2)$$
$$= D(E(D(C1,\ K1),\ K2)$$

得到的解密数据 M 输出给显示装置 56 等.

设备驱动程序为了与使用操作系统的计算机相适应, 或者在作为对象的设备已被改进的情况下, 一般要改变其规格参数.

通过将再加密/再解密处理和密钥的管理功能装入这样的设备驱动程序, 容易将这些功能装入操作系统的核心部. 此外, 通过在使用固定密钥 K0 再加密之前使用第 2 可变密钥 K2 进行再加密, 即使固定密钥 K0 被破译, 因数据还可以通过第 2 可变密钥 K2 加密, 所以, 进一步破译第 2 可变密钥 K2 来进行加密数据的解密就变得十分困难.

若第 2 可变密钥多次反复使用, 则有被破译的危险. 这时, 恰当的做法是, 象特开平 8－185448 号公报 (EP0704785A2, USSN08/536749) 所述的那样, 废弃第 2 可变密钥 K2, 当有必要解密时再重新生成.

此外, 为安全起见, K0、K1、K2 也可以使用不同的密码算法密钥.

这样的动作通过使固定方式加密/解密装置 57 是具有 CPU 和系统总线的子计算机结构就能够容易实现.

在迄今为止说明的实施例中, 除第 1 可变密钥 K1 之外, 还使用第 2 可变密钥 K2 和内藏固定密钥 K0. 在后面说明的实施例中, 通过增加使用第 3 可变密钥 K3 可以更加牢固地进行数字音像资料的著作权管理.

根据图 8 说明作为第 1 实施例的变形例的第 6 实施例的机顶盒的构成及用该机顶盒进行的数字数据的保护方法.

再有，该实施例的机顶盒也和第 1 实施例的机顶盒的情况一样，省略了与加密/解密无直接关系的外围电路、例如放大单元和压缩/解压缩单元的说明。

该第 6 实施例的机顶盒与第 1 实施例的机顶盒的不同之点在于：区别解密数据 M 保存在内藏于机顶盒的或专用的硬盘等保存媒体 81 中的情况和解密数据 M 保存在外部装置 82 中的作为可移动媒体的 DVDRAM 等中或经由网络向外部转送的情况。

因此，除内藏固定密钥方式加密/解密单元 15 之外还设置可变密钥方式加密单元 80；当拥有著作权的加密数据保存在内藏于机顶盒的或专用的硬盘等保存媒体 81 中时，用内藏固定密钥 KO 进行再再加密，当保存在作为可移动媒体的 DVDRAM 等中或经由网络向外部转送时，不使用内藏固定密钥 KO 而使用第 3 可变密钥 K3 进行再再加密。

在该图中，11 是由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据，为了防止非法使用，使用第 1 可变密钥 K1 进行加密，

C1 = E（M, K1）

并供给机顶盒 12.

在已供给加密数字数据 C1 的机顶盒 12 中，使用从密钥中心得到的第 1 可变密钥 K1，在解密单元 13 中对加密数字数据 C1 进行解密，

M = D（C1, K1）

得到的解密数据 M 向显示装置 14 等输出。

当拥有著作权的解密数据 M 保存在内藏于机顶盒的或专用的硬盘等保存媒体 81 中或保存在作为可移动媒体的 DVDRAM 等中或经由网络向外部传送时，在可变密钥方式加密/解密单元 19 的加密单元 20 中，使用从密钥中心得到的或机顶盒 12 内生成的第 2 可变密钥 K2 对解密数据 M 进行再加密，

A2: C2 = E（M, K2）

= E（D（C1, K1）, K2）

当再加密数据 C2 保存在内藏于机顶盒 12 或机顶盒 12 专用的硬盘等保存媒体 81 中时，在固定密钥方式加密/解密单元 15 的加密单元 16 中，使用内藏在内藏固定密钥方式加密/解密单元 15 中的固定密码密钥 KO 对再加密数据 C2 进行再再加密，

A2-0: C2-0 = E (C2, K0)

= E (E (D (C1, K1), K2), K0)

并作为再再加密数据 C2-0 保存在保存媒体 81 等中.

当利用保存媒体 81 保存的再再加密数据 C2-0 时，在内藏的固定密钥方式加密/解密单元 15 的解密单元 17 中，对从保存媒体 81 中读出的再加密数据 C2-0，使用内藏在内藏固定密钥方式加密/解密单元 15 中的固定密码密钥 K0 进行解密，

习 2: C2 = D (C2-0, K0)

= D (E (E (D (C1, K1), K2), K0)

= E (E (D (C1, K1), K2)

进而，在可变密钥方式加密/解密单元 19 的解密单元 21 中，对再解密数据 C2，使用可变密钥 K2 进行解密，

习: M = D (C2, K2)

= D (E (D (C1, K1), K2)

解密数据 M 输出给显示装置 14 等.

这时，为了保证安全，也可以构成为：当经由图中虚线所示路径从保存媒体 81 中读出再加密数据 C2-0 时，保存媒体 81 中的再加密数据 C2-0 被删去，使用可变密钥 K2 和内藏固定密码密钥 K0 再保存已再加密了的数据.

当再加密数据 C2 保存在外部装置 82 的可移动媒体 DVDRAM 中或经由网络向外部转送时，在可变密钥方式加密单元 80 中，使用从密钥中心得到的或机顶盒 12 内生成的第 3 可变密钥 K3 对再加密数据 C2 进行再再加密，

A2-3: C2-3 = E (C2, K3)

= E (E (M, K2), K3)

当利用经由外部装置 82 的再再加密数据 C2-3 时，在可变密钥方式加密/解密单元 83 的解密单元 84 中，使用党 3 可变密钥 K3 对再再加密数据 C2-3 进行解密，

习 2: C2 = D (C2-3, K3)

= D (E (M, K2), K3), K3)

= E (M, K2)

进而，在可变密钥方式加密/解密单元 83 的解密单元 85 中，对得到

的再加密数据 C2，使用第 2 可变密钥 K2 进行解密，

∃: M = D(C2, K2)

= D(E(M, K2), K2)

得到的解密数据 M 输出给显示装置 86 等.

这样的动作通过在机顶盒 12 内设置具有 CPU 和系统总线的子计算机结构就能够容易实现.

根据图 9 说明作为第 6 实施例的变形例的第 7 实施例的机顶盒的构成及用该机顶盒进行的数字数据的保护方法.

再有，该实施例的机顶盒也和第 6 实施例的机顶盒的情况一样，省略了与加密/解密无直接关系的外围电路、例如放大单元和压缩/解压缩单元的说明.

该第 7 实施例的机顶盒与第 6 实施例的机顶盒的不同之点在于：使用固定密钥 K0 进行加密/解密的固定密钥方式加密/解密单元 15 和使用第 2 可变密钥 K2 进行加密/解密的可变密钥方式加密/解密单元 19 的插入位置互相置换，因为是保存在外部装置 82 中的作为可移动媒体的 DVDRAM 等中或经由网络向外部转送的情况，所以，进而设置使用第 2 可变密钥 K2 进行加密/解密的可变密钥方式加密单元 87.

为了防止非法使用，由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据 11 使用第 1 可变密钥 K1 进行加密，

C1 = E(M, K1)

并作为数字数据 C1 供给机顶盒 12.

在已供给加密数字数据 C1 的机顶盒 12 中，使用从密钥中心得到的第 1 可变密钥 K1，在解密单元 13 中对加密数字数据 C1 进行解密，

M = D(C1, K1)

得到的解密数据 M 向显示装置 14 等输出.

当拥有著作权的解密数据 M 保存在内藏于机顶盒的或专用的硬盘等保存媒体 81 中时，在美内藏固定密钥方式加密/解密单元 15 中，使用固定密码密钥 K0 对再加密数据 C0 进行再加密，

A0: C0 = E(M, K0)

= E(D(C1, K1), K0)

在可变密钥方式加密/解密单元 19 的加密单元 20 中，使用从密

钥中心得到的或机顶盒 12 内生成的第 2 可变密钥 K2 进行再再加密，

A0-2: C0-2 = E (C0, K2)

= E (E (M, K0), K2)

并作为再再加密数据 C0-2 保存在保存媒体 81 等中.

当利用保存媒体 81 保存的再再加密数据 C0-2 时，在可变密钥方式加密/解密单元 19 的解密单元 21 中，对从保存媒体 81 中读出的再再加密数据 C0-2，使用第 2 可变密钥 K2 进行再解密，

∃ 0: C0 = D (C0-2, K2)

= D (E (C0, K2), K2)

进而，在固定密钥方式加密/解密单元 15 的解密单元 17 中，对再解密数据 C0，使用固定密钥 K0 进行再再解密，

∃: M = D (C0, K0)

= D (E (M, K0), K0)

得到的解密数据 M 输出给显示装置 14 等.

这时，为了保证安全，也可以构成为：当经由图中虚线所示路径从保存媒体 81 中读出再加密数据 C0-2 时，保存媒体 81 中的再加密数据 C0-2 被删去，使用第 2 可变密钥 K2 和固定密钥 K0 再保存已再加密了的数据.

当解密数据 M 保存在外部装置 82 的可移动媒体 DVDRAM 中或经由网络向外部转送时，在可变密钥方式加密单元 80 中，使用从密钥中心得到的或机顶盒 12 内生成的第 3 可变密钥 K3 将解密数据 M 再加密成再加密数据 C3.

A3: C3 = E (M, K3)

= E (D (C1, K1), K3)

在可变密钥方式加密单元 87 中，使用从密钥中心得到的或机顶盒 12 内生成的第 2 可变密钥 K2 将再加密数据 C3 加密成再再加密数据 C3-2，

A3-2: C3-2 = E (C3, K2)

= E (E (D (C1, K1), K3), K2)

再再加密数据 C3-2 保存在 DVDRAM 中或经由网络转送给外部装置 82.

当利用经由外部装置 82 的再再加密数据 C3-2 时，在可变密钥方式加密/解密单元 83 的解密单元 84 中，对再再加密数据 C3-2，使用

第 3 可变密钥 K3 进行解密，

$$\exists\ 3:\ C3 = D(C3\text{-}2,\ K2)$$
$$= D(E(C3,\ K2),\ K2)$$

进而，在可变密钥方式加密/解密单元 83 的解密单元 85 中，对得到的再再加密数据 C2，使用第 3 可变密钥 K3 进行解密，

$$\exists:\ M = D(C3,\ K3)$$
$$= D(E(M,\ K3),\ K3)$$

得到的解密数据 M 输出给显示装置 86 等.

再有，该实施例在可变密钥方式加密单元 80 中使用第 3 可变密钥 K3，在可变密钥方式加密单元 87 中使用第 2 可变密钥 K2，但也可以将该顺序颠倒过来.

此外，也可以构成为在可变密钥方式加密/解密单元 19 的加密单元 20 中执行可变密钥方式加密单元 87 的功能.

进而，虽然说明了加密单元 16 和解密单元 17 包含在固定密钥方式加密/解密单元 15 中、加密单元 20 和解密单元 21 包含在可变密钥方式加密/解密单元 19 中的情况，当然也可以将这些单元 16、17、20、21 分离开来设置.

这样的动作通过在机顶盒 12 内设置具有 CPU 和系统总线的子计算机结构就能够容易实现.

说明适用于使用了个人计算机的装置的实施例的变形实施例.

图 10 所示的第 8 实施例是图 5 所示的第 4 实施例的变形例，但省略了该实施例构成中的与第 4 实施例共同的部分的说明.

该第 8 实施例与第 4 实施例的不同点在于：区别解密数据 M 保存在内藏于计算机的或专用的硬盘等保存媒体 81 中的情况和解密数据 M 保存在作为可移动媒体 92 的 DVDRAM 等中或经由网络 93 向外部转送的情况.

因此，除固定方式加密/解密单元 89 之外，作为硬件 88 还设有可变密钥方式加密/解密单元 90 及 91，拥有著作权的解密数据保存在内藏于计算机的或专用的硬盘等保存媒体中，在这种情况下，经由盘驱动程序 67 在加密/解密部 90 中使用第 3 可变密钥 K3 进行再再加密和解密，在经由网络 93 向外部转送的情况下，经由网络驱动程序 68 在可变密钥方式加密/解密单元 91 中使用第 3 可变密钥 K3 进行再再

加密和解密.

与图 2 所示的第 1 实施例的情况一样，为了防止非法使用，由数字地面波广播、数字 CATV 广播和数字卫星广播等广播设备、因特网等网络设备或 DVD、CD 等数字保存媒体提供的数字数据 11 使用第 1 可变密钥 K1 进行加密，

C1, = E（M, K1）

并提供，供给的加密数字数据 C1 通过和加密数字数据 C1 相同的路径或和加密数字数据 C1 不同的路径，使用从密钥中心提供的第 1 可变密钥 K1，由操作系统服务部 52 进行解密，

M = D（C1, K1）

解密数据 M 向显示装置 56 等输出.

当解密数据M保存在内藏于计算机的或专用的硬盘等保存媒体 81 中、或保存在 DVDRAM 等媒体中或经由网络向外部转送时，在滤波器驱动程序 66 中，使用从密钥中心得到的或操作系统服务部 52 内生成的第 2 可变密钥 K2 对解密数据 M 进行再加密.

A2: C2 = E（M, K2）= E（D（C1, K1）, K2）

进而，当再加密数据 C2 保存在内藏于计算机的或专用的硬盘等保存媒体 81 中时，在硬件 88 内的加密/解密单元 89 中，使用固定密钥 K0 对再加密数据 C2 进行再再加密，

A2-0: C2-0 = E（C2, K0）= E（E（D（C1, K1）, K2）, K0）

并作为再再加密数据 C2-0 保存在硬盘 81 等中.

当利用保存媒体 81 保存的再再加密数据 C2-0 时，在硬件 88 内的加密/解密单元 89 中，对从保存媒体 81 中读出的再加密数据 C2-0，使用固定密码密钥 K0 进行再解密，

ヨ 2: C2 = E（C2-0, K0）= D（E（E（D（C1, K1）, K2）, K0）

进而，在具有加密/解密功能的滤波器驱动程序 66 中，对再解密数据 C2，使用第 2 可变密钥 K2 进行解密，

ヨ: M = D（C2, K2）= D（E（D（C1, K1）, K2）

解密数据 M 用于利用计算机的操作系统向显示装置 56 等输出等.

此外，当再加密数据 C2 保存在 DVDRAM 等可移动媒体中时，在可变密钥方式加密/解密单元 90 中，使用第 2 可变密钥 K2 将对再加密数据 C2 进行再再加密，

A2-3: C2-3 = E(C2, K3) = E(E(D(C1, K1), K2), K3)
作为再再加密数据 C2-3 保存在 DVDRAM 等可移动媒体中.

当利用保存在可移动媒体 92 中的再再加密数据 C2-3 时，在硬件内的加密/解密单元 90 中，对从可移动媒体 92 中读出的再加密数据 C2-3，使用从密钥中心得到的或操作系统服务部 52 内生成的第 3 可变密钥 K3 进行再解密，

∃ 2: C2 = E(C2-3, K3) = D(E(E(D(C1, K1), K2), K3)
进而，在具有加密/解密功能的滤波器驱动程序 66 中，对再加密数据 C2，使用第 2 可变密钥 K2 进行解密，

∃: M = D(C2, K2) = D(E(D(C1, K1), K2)
解密数据 M 用于利用计算机的操作系统向显示装置 56 等输出等.

此外，当再加密数据 C2 经由网络 93 向外部转送时，在加密/解密单元 91 中，使用第 2 可变密钥 K2 对再加密数据 C2 进行再再加密，

A2-3: C2-3 = E(C2, K3) = E(E(D(C1, K1), K2), K3)
并作为再再加密数据 C2-3 经由网络 93 向外部转送.

当利用经由网络 88 从外部转送来的再再加密数据 C2-3 时，在加密/解密单元 91 中，对加密数据 C2-3，使用第 3 可变密钥 K3 进行再解密，

∃ 2: C2 = E(C2-3, K3) = D(E(E(D(C1, K1), K2), K3)
进而，在具有加密/解密功能的滤波器驱动程序 66 中，对再解密数据 C2，使用第 2 可变密钥 K2 进行解密，

∃: M = D(C2, K2) = D(E(D(C1, K1), K2)
解密数据 M 用于利用计算机的操作系统向显示装置 56 等输出等.

在该实施例中为说明方便起见，将加密/解密单元 90 和加密/解密单元 91 作为两个独立的装置进行说明，当然，也可以将它们作为一个装置.

此外，这样的加密/解密管理在操作系统 51 内的 HAL55 中优先于其它任务，利用前面说明了的实时 OS(RTOS)进行.

这样的动作通过使硬件结构是具有 CPU 和系统总线的子计算机结构就能够容易实现.

图 11 所示的是使用了具有进行第 8 实施例的可变密钥方式加密/解密处理的滤波器驱动程序 66 的 I/O 管理微核心模块 64 的加密/解

密处理的具体结构.

I/O管理微核心模块64从上位层到下位层配置有文件系统驱动程序69、中间驱动程序70和作为设备驱动程序的盘驱动程序67及网络驱动程序68，必要时，在文件系统驱动程序69的上位层或中间驱动程序70和设备驱动程序之间插入进行可变密钥方式加密/解密处理的滤波器驱动程序66A或滤波器驱动程序66B.

因可以在这些滤波器驱动程序66A和滤波器驱动程序66B中进行再加密/再解密处理和密钥的管理，故在该实施例中，再加密/再解密处理和密钥的管理在滤波器驱动程序66A或滤波器驱动程序66B中进行.

当拥有著作权的解密数据M保存在内藏或专用的硬盘等保存媒体或数字视盘DVDRAM等可移动媒体中或经由网络向外部传送时，在滤波器驱动程序66A或滤波器驱动程序66B中，使用从密钥中心得到的或I/O管理微核心模块内生成的第2可变密钥K2对加密数据M进行再加密，

A2: C2 = E(M, K2) = E(D(C1, K1), K2)

进而，当再加密数据C2保存在内藏于计算机或专用的保存媒体81中时，在硬件88内的加密/解密单元89中，使用固定密钥KO对再加密数据C2进行再再加密，

A2-O: C2-O = E(C2, KO) = E(E(D(C1, K1), K2), KO)

并作为再再加密数据C2-O保存在硬盘81中.

当利用保存媒体81保存的再再加密数据C2-O时，在硬件88内的加密/解密单元89中，对从保存媒体81中读出的再加密数据C2-O，使用固定密钥KO进行解密，

∃2: C2 = E(C2-O, KO) = D(E(E(D(C1, K1), K2), KO)

进而，在具有/解密功能的滤波器驱动程序66中，对再解密数据C2，使用第2可变密钥K2进行解密，

∃: M = D(C2, K2) = D(E(D(C1, K1), K2)

解密数据M用于利用计算机的操作系统向显示装置56等输出等.

此外，当再加密数据C2保存在DVDRAM等可移动媒体中时，在硬件88内的加密/解密单元90中，使用从密钥中心得到的或I/O管理微核心64内生成的第3可变密钥K3对再加密数据C2进行再再加密，

A2-3: C2-3 = E (C2, K3) = E (E (D (C1, K1), K2), K3)

作为再再加密数据 C2-3 保存在 DVDRAM 等可移动媒体中.

当利用保存在可移动媒体 92 中的再再加密数据 C2-3 时，在硬件 88 内的加密/解密单元 90 中，对从可移动媒体 92 中读出的再加密数据 C2-3，使用第 3 可变密钥 K3 进行再解密，

ヨ 2: C2 = E (C2-3, K3) = D (E (E (D (C1, K1), K2), K3)

进而，在具有加密/解密功能的滤波器驱动程序 66 中，对再加密数据 C2，使用第 2 可变密钥 K2 进行解密，

ヨ: M = D (C2, K2) = D (E (D (C1, K1), K2)

解密数据 M 用于利用计算机的操作系统向显示装置 56 等输出等.

此外，当再加密数据 C2 经由网络 93 向外部转送时，在加密/解密单元 91 中，使用第 2 可变密钥 K2 对再加密数据 C2 进行再再加密，

A2-3: C2-3 = E (C2, K3) = E (E (D (C1, K1), K2), K3)

并作为再再加密数据 C2-3 经由网络 93 向外部转送.

当利用经由网络 93 从外部转送来的再再加密数据 C2-3 时，在加密/解密单元 91 中，对加密数据 C2-3，使用第 3 可变密钥 K3 进行再解密，

ヨ 2: C2 = E (C2-3, K3) = D (E (E (D (C1, K1), K2), K3)

进而，在具有加密/解密功能的滤波器驱动程序 66 中，对再解密数据 C2，使用第 2 可变密钥 K2 进行解密，

ヨ: M = D (C2, K2) = D (E (D (C1, K1), K2)

解密数据 M 用于利用计算机的操作系统向显示装置 56 等输出等.

设备驱动程序为了与使用操作系统的计算机相适应，或者在作为对象的设备已被改进的情况下，一般要改变其规格参数.

通过将再加密/再解密处理和密钥的管理功能装入这样的设备驱动程序，容易将这些功能装入操作系统的核心部. 此外，通过在使用固定密钥 KO 再加密之前使用第 2 可变密钥 K2 进行再加密，即使固定密钥 KO 被破译，因数据还可以通过第 2 可变密钥 K2 加密，所以，进一步破译第 2 可变密钥 K2 来进行加密数据的解密就变得十分困难.

此外，第 2 可变密钥 K2 最初用于再加密，而在使用固定密钥 KO 之后，又在最后被使用，所以，密钥的安全性高，而且，因最初被使用故能强有力地支配加密数据.

若第 2 可变密钥多次反复使用，则有被破译的危险．这时，恰当的做法是，象特开平 8－185448 号公报（EP0704785A2，USSN08/536749）所述的那样，废弃第 2 可变密钥 K2，当有必要解密时再重新生成．

此外，为安全起见，K1、K2、K3、K0 也可以使用不同的密码算法密钥．

这样的动作通过使硬件 88 是具有 CPU 和系统总线的子计算机结构就能够容易实现．

为了这样来进行数字数据的再加密/再解密，有必要对数字数据附加用来识别限制数字数据的保存或转送的符号．而且，当对数字数据不进行加工而保存或转送时，利用前面所述的再加密/再解密方法及其装置，可以防止数字数据的非法利用．

但是，当已对数字数据进行了加工时，有可能丢失用来识别限制保存或转送的符号．

在这样的情况下，只要使用针对该装置的固有的密钥（主密钥）对所有的数据进行再加密/再解密即可．

这样一来，即使是使用剪切和粘贴等方法加工了的数字数据，通过再加密/再解密也能够防止其非法利用．

再有，这时使用主密钥进行再加密/再解密的数字数据只限于没有附加用来识别限制保存或转送的符号的数据，对于附加了用来识别限制保存或转送的符号的数字数据，可以利用前面所述的再加密/再解密方法及其装置进行再加密/再解密．

当通过机顶盒等专用装置来利用拥有著作权的已加密的数字数据时，比较容易实现非法保存、复制或转送的防止．此外，当通过计算机来利用拥有著作权的已加密的数字数据时，通过特开平 8－287014（USP5867579，EP0715241A2）所示的再加密/再解密装置或 USP5805706 所示的再加密/再解密装置，可以对保存、复制或转送已解密的数字数据进行管理．

但是，在计算机总线上存在用来显示或打印的已解密的数字数据，可以经由与总线连接的装置对已解密的数字数据进行保存、复制或转送．下面，说明可以防止出现该问题的著作权管理装置．

图 12 所示的是著作权管理装置的构成例，在该著作权管理装置

中，密码密钥使用第 1 可变密钥和第 2 可变密钥.

此外，为安全起见，著作权管理装置以子插件、PCMCIA 卡、IC 卡或 IC 组件的形态实现.

在该图中，101 是 CPU，在与 CPU101 连接的总线 102 上连接有 ROM103、RAM104、硬盘驱动器 105、软盘驱动器 106、CD—ROM 驱动器 107 和调制解调器 108 等.

109 是著作权管理装置，著作权管理装置 109 具有加密/解密单元 110 及视频接口 113、音频接口 114 和打印接口 115.

视频接口 113、音频接口 114 和打印接口 115 在计算机的外部分别与显示装置 116、扬声器 117 和打印机 118 连接.

加密/解密单元 110 具有解密单元 111 和加密单元 112.

加密/解密单元 110 的解密单元 111 和加密单元 112 都与计算机的系统总线 102 连接，解密单元 111 进而与视频接口 113、音频接口 114 和打印接口 115 连接.

这样的结构通过使著作权管理装置 109 是具有 CPU 和系统总线的子计算机结构就能够容易实现.

已解密的数字数据经硬盘驱动器 105 保存、软盘驱动器 106 复制或调制解调器 108 转送时，在再加密单元 115 中，使用第 2 可变密钥 K2 进行再加密，

$$A2:\ C2 = E(M, K2)$$
$$= E(D(C1, K1), K2)$$

再加密数字数据 C2 供给系统总线 102，由硬盘驱动器 105 保存、软盘驱动器 106 复制或调制解调器 108 转送.

使用第 1 可变密钥 K1 加密后的数字数据 C1 从系统总线 102 供给解密单元 111，使用第 1 可变密钥 K1 进行解密.

$$M = D(C1, K1)$$

当已解密的数字数据 M 输出给显示装置 116 或扬声器 117 时，在著作权管理装置 109 内的视频接口 113、音频接口 114 中转换成模拟信号并以规定的信号形式输出.

当已解密的数字数据 M 输出给打印机 118 时，经打印机接口 115 输出打印数据.

若使用该著作权管理装置 109，输出给打印机的数据以外的解密

数字数据在著作权管理装置 109 之外不存在．而且，因向打印机输出的数据是静止数据，故动画或声音等数字数据在著作权管理装置 109 之外不存在．

在计算机内，除已解密的数字数据之外，还存在未解密的数字数据．

为了区别这样的非解密数字数据和解密数字数据，必须分别设置视频接口、音频接口和打印接口，装置变得昂贵而复杂．为了避免这样的情况，利用著作权管理装置 109 的视频接口 113、音频接口 114 也可以处理非解密数字数据．

图 13 所示的是著作权管理装置的另一构成例，在该著作权管理装置中，密码密钥除第 1 可变密钥和第 2 可变密钥之外还使用固定密钥．

此外，为安全起见，著作权管理装置以子插件、PCMCIA 卡、IC 卡或 IC 组件的形态实现．

在该图中，101 是 CPU，在与 CPU101 连接的总线 102 上连接有 ROM103、RAM104、硬盘驱动器 105、软盘驱动器 106、CD—ROM 驱动器 107 和调制解调器 108 等．

120 是著作权管理装置，著作权管理装置 120 除解密/再加密单元 110 之外还具有固定密钥加密单元 121 及加密视频接口 122、加密音频接口 123 和加密打印接口 124．

解密/再加密单元 110 具有解密单元 111 和再加密单元 112．

此外，加密视频接口 122、加密音频接口 13 和加密打印接口 124 在计算机的外部分别与加密数字图像显示装置 125、加密数据声音重放装置 126 和加密数据打印机 127 连接．

解密/再加密单元 110 的解密单元 111 和再加密单元 112 都与计算机的系统总线 102 连接，解密单元 111 进而与固定密钥加密单元 121 连接．

固定密钥加密单元 121 与加密视频接口 122、加密音频接口 123 和加密打印接口 124 连接．

加密视频接口 122 与加密数字图像显示装置 125 连接，加密音频接口 123 与加密数据声音重放装置 126 连接，加密打印接口 124 与加密数据打印机 127 连接．

这样的结构通过使著作权管理装置 109 是具有 CPU 和系统总线的子计算机结构就能够容易实现.

加密数字图像显示装置 125 具有与加密视频接口 122 连接的固定密钥解密装置 128、与固定密钥解密装置 128 连接的 D/A 变换器 131 和与 D/A 变换器 131 连接的显示装置 116.

加密数据声音重放装置 126 具有与加密音频接口 123 连接的固定密钥解密装置 129、与固定密钥解密装置 129 连接的 D/A 变换器 132 和与 D/A 变换器 132 连接的扬声器 117.

加密数据打印机 127 具有与加密打印机接口 124 连接的固定密钥解密装置 130、与固定密钥解密装置 130 连接的打印机 118.

再有，加密数据显示装置 125、加密数据声音重放装置 126 和加密数据打印机 127 当然还具有放大器等其它构件.

使用第 1 可变密钥 K1 加密后的数字数据 C1 从系统总线 102 供给解密单元 111，使用第 1 可变密钥 K1 进行解密.

$$M = D(C1, K1)$$

当已解密的数字数据 M 经硬盘驱动器 105 保存、软盘驱动器 106 复制或调制解调器 108 转送时，在再加密单元 115 中，使用第 2 可变密钥 K2 进行再加密，

$$A2:\ C2 = E(M, K2)$$
$$= E(D(C1, K1), K2)$$

再加密数字数据 C2 供给系统总线 102，由硬盘驱动器 105 保存、软盘驱动器 106 复制或调制解调器 108 转送.

当已解密的数字数据 M 输出给加密显示装置 125、加密数据声音重放装置 126 或加密数据打印机 127 时，在著作权管理装置 120 内的固定加密单元 121 中中使用固定密钥 K0 进行再加密，

$$A0:\ C0 = E(M, K0)$$
$$= E(D(C1, K1), K0)$$

再加密数字数据 C0 在加密视频接口 122、加密音频接口 123 和加密打印接口 124 中编组并作为加密显示信号 Cd0、加密声音信号 Ca0 和加密打印信号 Cp0 输出.

从加密视频接口 122 向加密数据显示装置 125 输入的加密显示信号 Cd0 在固定密钥解密装置 128 中使用固定密钥 K0 进行解密，

Md = D (CdO, KO)

解密显示信号 Md 在 D/A 变换器 131 中变换成可显示的模拟信号，并在显示装置 116 中显示.

再有，当该显示装置 116 是可以直接显示数字数据的数据显示装置时，就不需要 D/A 变换器 131.

从加密音频接口 123 向加密数据声音重放装置 126 输入的加密声音信号 CaO 在固定密钥解密装置 129 中使用固定密钥 KO 进行解密，

Ma = D (CaO, KO)

解密声音信号 Ma 在 D/A 变换器 132 中变换成可重放的模拟信号，并利用扬声器 117 重放声音.

从加密打印机接口 124 输向加密数据打印机 127 输入的加密打印信号 CpO 在固定密钥解密装置 130 中使用固定密钥 KO 进行解密，

Mp = D (CpO, KO)

解密打印信号 Mp 通过打印机 118 打印.

若使用该著作权管理装置 120，所有的解密数据都不在著作权管理装置 120 之外存在.

在计算机内，除已解密的数字数据之外，还存在未解密的数字数据.

为了区别这样的非解密数字数据和解密数字数据，必须分别设置视频接口、音频接口和打印接口，装置变得昂贵而复杂. 为了避免这样的情况，可以利用著作权管理装置 120 的固定密钥再加密单元 121 处理非加密数字数据.

图 14 所示的是著作权管理装置的又一构成例，在该著作权管理装置中，固定密钥加密单元设在视频接口、音频接口和打印机接口之后.

为安全起见，著作权管理装置以子插件、PCMCIA 卡、IC 卡或 IC 组件的形态实现.

在该图中，101 是 CPU，在与 CPU101 连接的总线 102 上连接有 ROM103、RAM104、硬盘驱动器 105、软盘驱动器 106、CD—ROM 驱动器 107 和调制解调器 108 等.

140 是著作权管理装置，著作权管理装置 140 除解密/再加密单元 110 之外还具有视频接口 131、音频接口 132、打印接口 133 和固定

密钥加密单元 134.

解密/再加密单元 110 具有解密单元 111 和再加密单元 112.

此外，固定密钥加密单元 134 具有视频固定密钥加密单元 135、音频固定密钥加密单元 136 和打印机用固定密钥加密单元 137，但这些视频固定密钥加密单元 135、音频固定密钥加密单元 136 和打印机用固定密钥加密单元 137，若其具有足够的加密能力，也可以只使用一个.

解密/再加密单元 110 的解密单元 111 和再加密单元 112 都与计算机的系统总线 102 连接，解密单元 111 进而与视频接口 131、音频接口 132、打印接口 133 连接，这些接口又与视频固定密钥加密单元 135、音频固定密钥加密单元 136 和打印机用固定密钥加密单元 137 连接.

视频固定密钥加密单元 135、音频固定密钥加密单元 136 和打印机用固定密钥加密单元 137 与计算机外部的加密数字图像显示装置 125、加密数据声音重放装置 126 和加密数据打印机 127 连接.

这样的结构通过使著作权管理装置 140 是具有 CPU 和系统总线的子计算机结构就能够容易实现.

加密数字图像显示装置 125 具有与视频固定密钥加密单元 135 连接的固定密钥解密装置 128、与固定密钥解密装置 128 连接的 D/A 变换器 131 和与 D/A 变换器 131 连接的显示装置 116.

加密数据声音重放装置 126 具有与音频固定密钥加密单元 136 连接的固定密钥解密装置 129、与固定密钥解密装置 129 连接的 D/A 变换器 132 和与 D/A 变换器 132 连接的扬声器 117.

加密数据打印机 127 具有与打印机用固定密钥加密单元 137 连接的固定密钥解密装置 130、与固定密钥解密装置 130 连接的打印机 118.

再有，加密数据显示装置 125、加密数据声音重放装置 126 和加密数据打印机 127 当然还具有放大器等其它构件.

使用第 1 可变密钥 K1 加密后的数字数据 C1 从系统总线 102 供给解密单元 111，使用第 1 可变密钥 K1 进行解密.

M = D（C1，K1）

当已解密的数字数据 M 经硬盘驱动器 105 保存、软盘驱动器 106

复制或调制解调器 108 转送时，在再加密单元 115 中，使用第 2 可变密钥 K2 进行再加密，

A2: C2 = E（M, K2）
= E（D（C1, K1）, K2）

再加密数字数据 C2 供给系统总线 102，由硬盘驱动器 105 保存、软盘驱动器 106 复制或调制解调器 108 转送.

当解密的数字数据 M 输出给加密数据显示装置 125、加密数据声音重放装置 126 或加密数据打印机 127 时，在著作权管理装置 140 内的视频接口 131、音频接口 132、打印接口 133 中，解密数字数据 M 编组成适合于各显示装置 116、声音重放装置 117 和打印机 118 的数字数据 Md、Ma 和 Mp，在各个显示用固定密钥加密单元 135、声音重放用固定密钥加密单元 136 和打印机用固定密钥加密单元 137 中，使用固定密钥 K0 对这些数字数据进行加密，

Cd0 = E（Md, K0）
Ca0 = E（Ma, K0）
Cp0 = E（Mp, K0）

并作为加密显示信号 Cd0、加密声音重放信号 Ca0 和加密打印信号 Cp0 输出.

从显示用固定密钥加密单元 135 向加密数据显示装置 125 输入的加密显示信号 Cd0 在固定密钥解密装置 128 中，使用固定密钥 K0 进行解密，

Md = D（Cd0, K0）

解密显示信号 Md 在 D/A 变换器 131 中转换成可显示的模拟信号，在显示装置 116 中显示.

再有，这时，当该显示装置 116 是可以直接显示数字数据的数字显示装置时，就不需要 D/A 变换器 131.

从声音重放用固定密钥加密单元 136 向加密数据声音重放装置 126 输入的加密声音信号 Ca0 在固定密钥解密装置 129 中使用固定密钥 K0 进行解密，

Ma = D（Ca0, K0）

解密声音信号 Ma 在 D/A 变换器 132 中变换成可重放的模拟信号，并利用扬声器 117 重放声音.

从打印机用固定密钥加密单元 137 向加密数据打印机 127 输入的加密打印信号 CpO 在固定密钥解密装置 130 中使用固定密钥 KO 进行解密，

Mp = D（CpO，KO）

解密打印信号 Mp 通过打印机 118 打印.

若使用该著作权管理装置 140，所有的解密数据都不在著作权管理装置 140 之外存在.

在计算机内，除已解密的数字数据之外，还存在未解密的数字数据.

为了区别这样的非解密数字数据和解密数字数据，必须分别设置视频接口、音频接口和打印接口，装置变得昂贵而复杂. 为了避免这样的情况，可以利用著作权管理装置 140 的视频接口 131、音频接口 132、打印接口 133 来处理非加密数字数据.

作为数字数据加密时使用的加密方式大多使用秘密密钥加密方式. 该秘密密钥方式的最普及的 DES（数据加密标准：Data Encryption Standard）将数据以 64 位为单位分成块进行加密/解密. 该块加密方式在秘密密钥方式中是一般的手法，其它的秘密密钥方式也采用. 若采用以快为单位进行加密/解密，可以实现高速加密/解密处理.

因此，将设在加密/解密单元内的加密单元和解密单元设置成多个，将数据块的加密/解密处理顺序分配给多个加密单元和解密单元去执行，再将得到的加密/解密执行结果按顺序合成.

作为该构成的附属效果，可以对每一个数据块使用不同的加密密钥，进而，可以对每一个数据块采用不同的加密方式. 这样一来，可以更牢靠地保护数字数据.

说 明 书 附 图

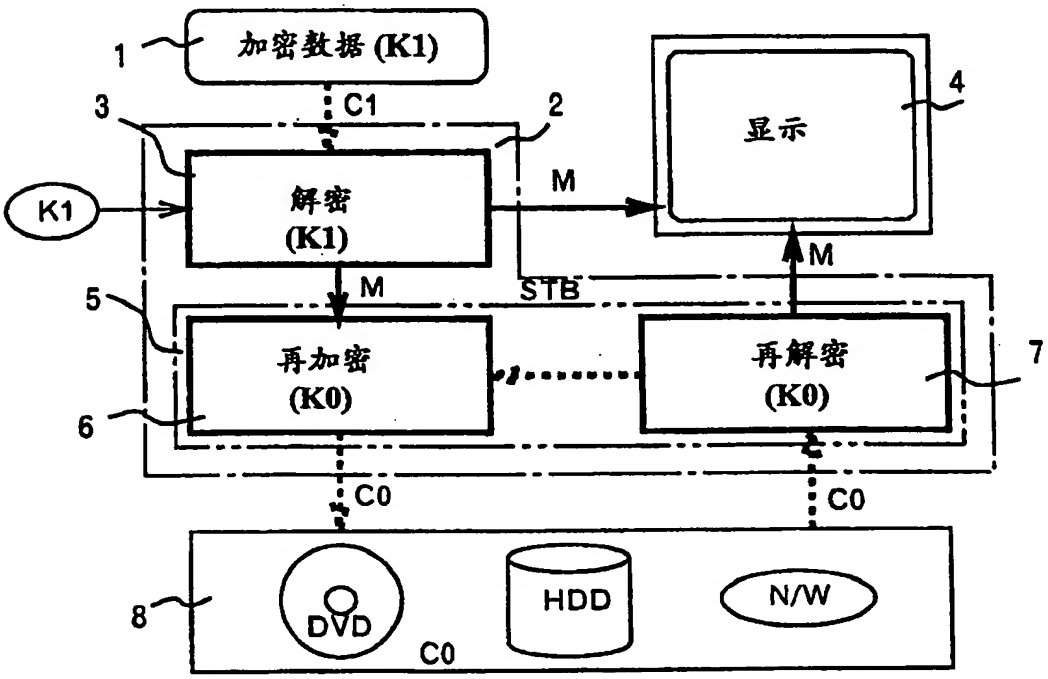

1
加密数据 (K1)
C1
3
2
4
显示
K1
解密
(K1)
M
M
M
STB
5
再加密
(K0)
再解密
(K0)
7
6
C0
C0
8
DVD
C0
HDD
N/W

图 1

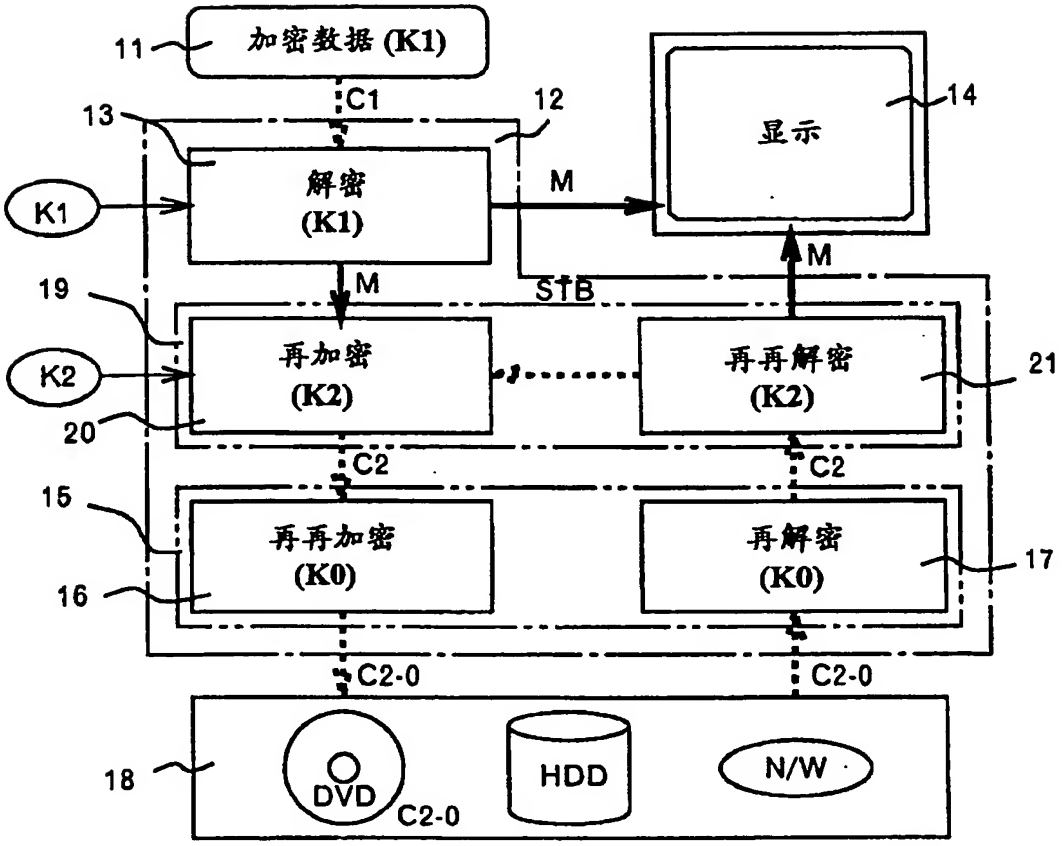

11
加密数据 (K1)
C1
12
13
显示
14
解密
(K1)
K1
M
M
M
STB
19
再加密
(K2)
再再解密
(K2)
21
K2
20
C2
C2
15
再再加密
(K0)
再解密
(K0)
17
16
C2-0
C2-0
18
DVD
C2-0
HDD
N/W

图 2

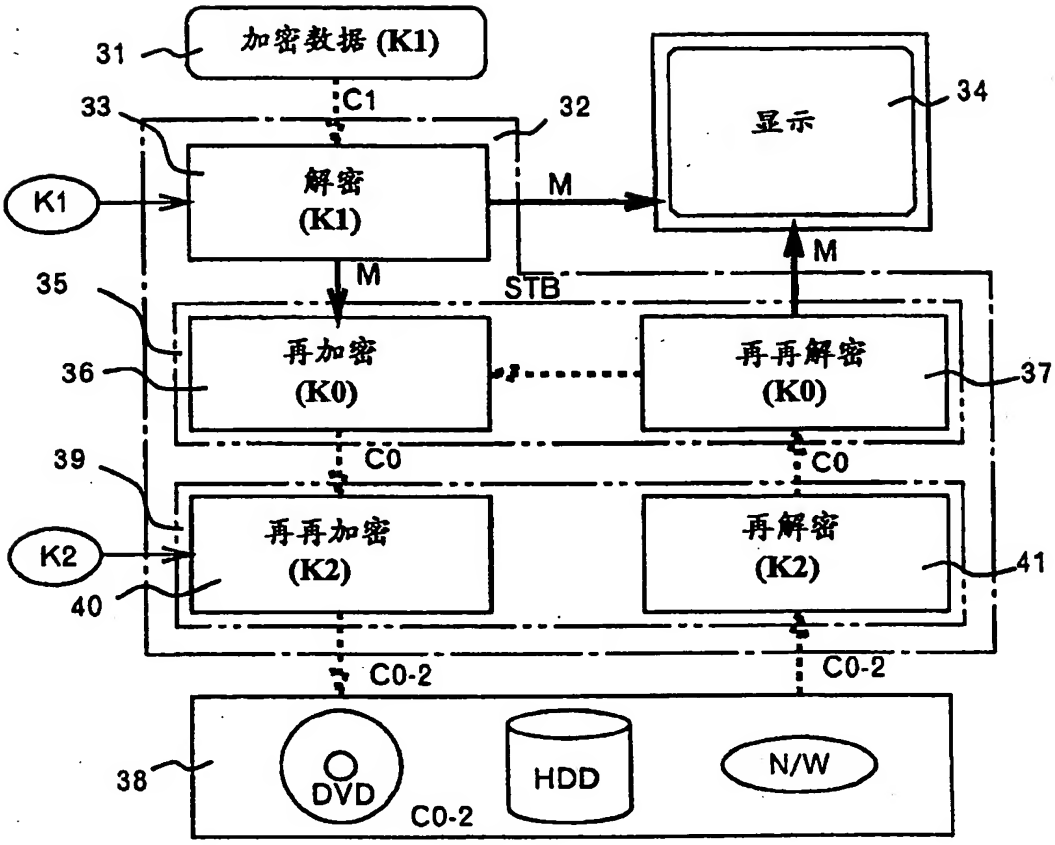

31
加密数据 (K1)
C1
33
32
显示
34
K1
解密
(K1)
M
M
M
STB
35
再加密
(K0)
36
再再解密
(K0)
37
C0
C0
39
K2
再再加密
(K2)
40
再解密
(K2)
41
C0-2
C0-2
38
DVD
C0-2
HDD
N/W

图 3

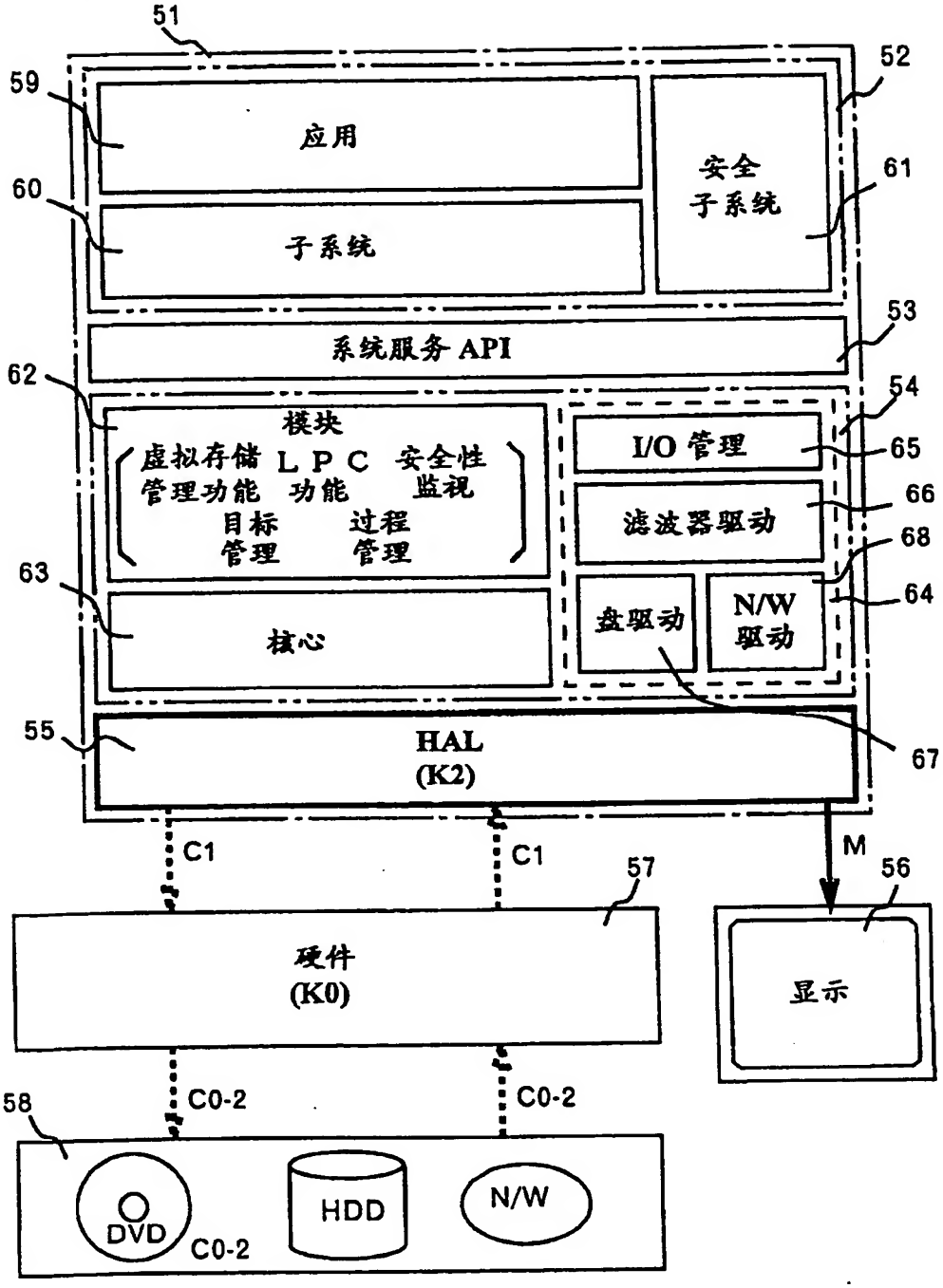

51
52
59
应用
安全
子系统
61
60
子系统
53
系统服务 API
62
模块
虚拟存储 L P C 安全性
管理功能 功能 监视
目标 过程
管理 管理
54
I/O 管理
65
66
滤波器驱动
68
63
核心
盘驱动
N/W
驱动
64
55
HAL
(K2)
67
C1
C1
M
57
56
硬件
(K0)
显示
C0-2
C0-2
58
DVD
C0-2
HDD
N/W

图 4

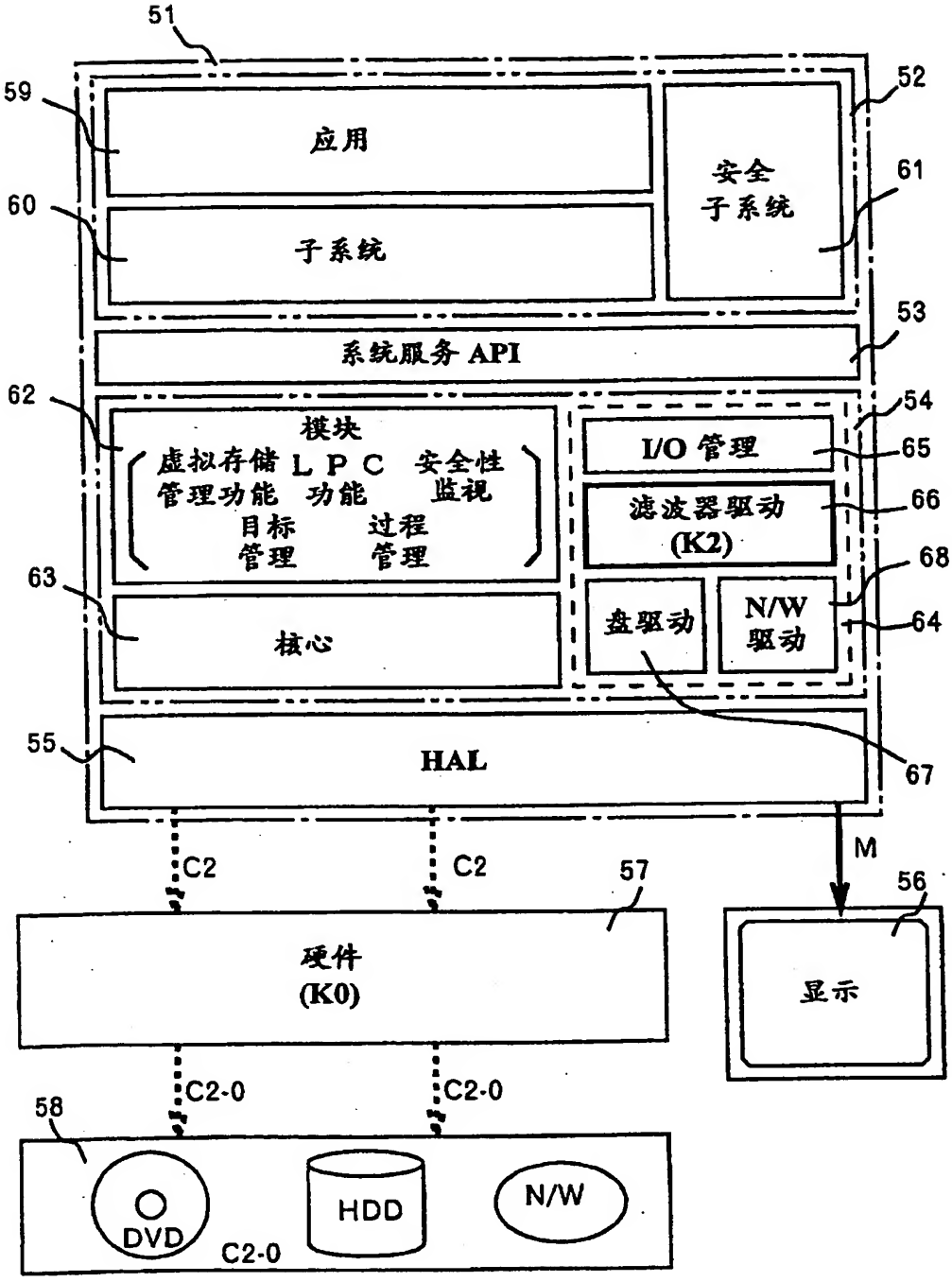

51
59
52
应用
安全
子系统
61
60
子系统
53
系统服务 API
62
54
模块
虚拟存储 L P C 安全性
管理功能 功能 监视
目标 过程
管理 管理
I/O 管理
65
滤波器驱动
(K2)
66
68
63
核心
盘驱动
N/W
驱动
64
55
HAL
67
M
C2
C2
57
56
硬件
(K0)
显示
C2-0
C2-0
58
DVD
C2-0
HDD
N/W

图 5

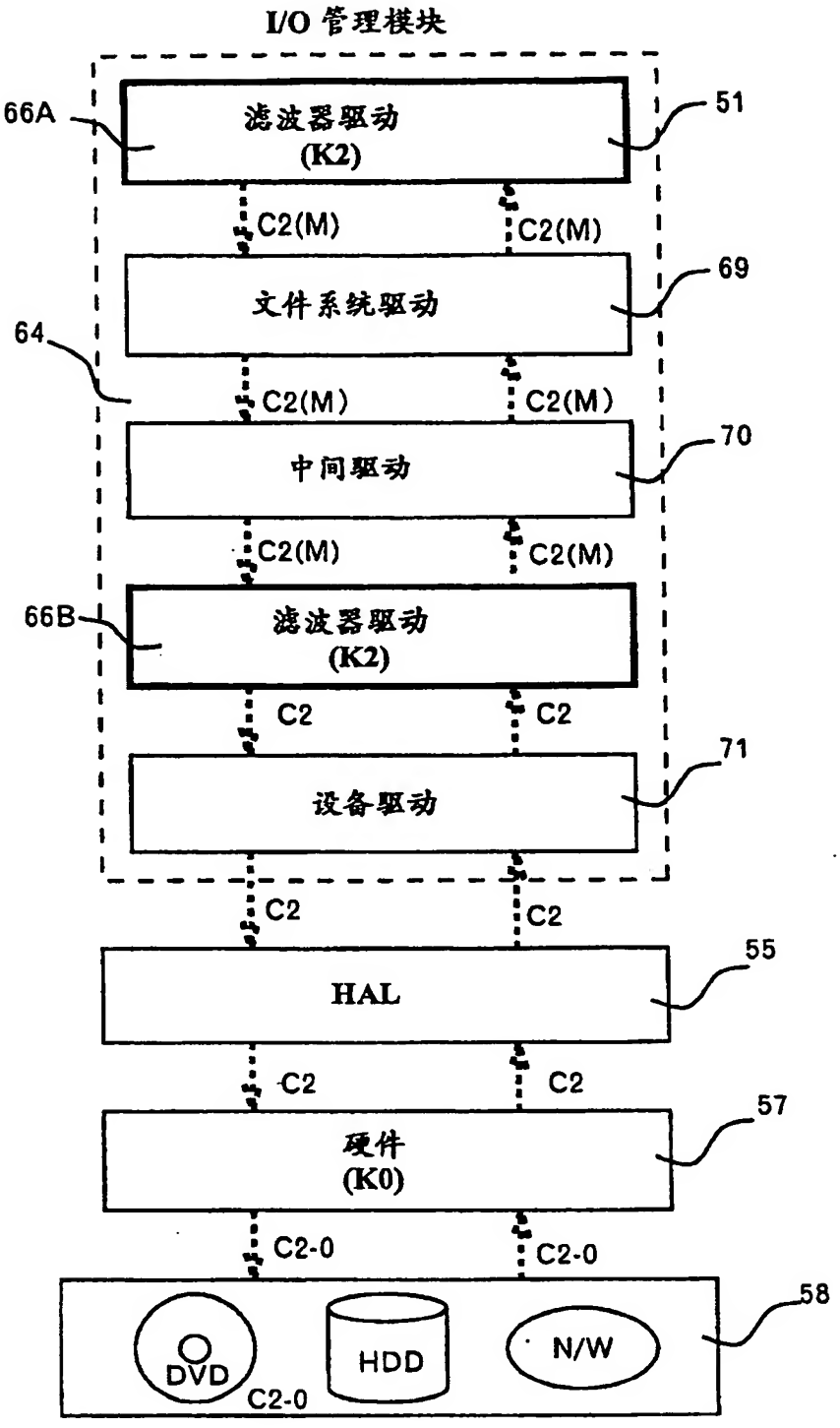

I/O 管理模块
66A
滤波器驱动
(K2)
51
C2(M)
C2(M)
文件系统驱动
69
64
C2(M)
C2(M)
中间驱动
70
C2(M)
C2(M)
66B
滤波器驱动
(K2)
C2
C2
设备驱动
71
C2
C2
HAL
55
C2
C2
硬件
(K0)
57
C2-0
C2-0
DVD
C2-0
HDD
N/W
58

图 6

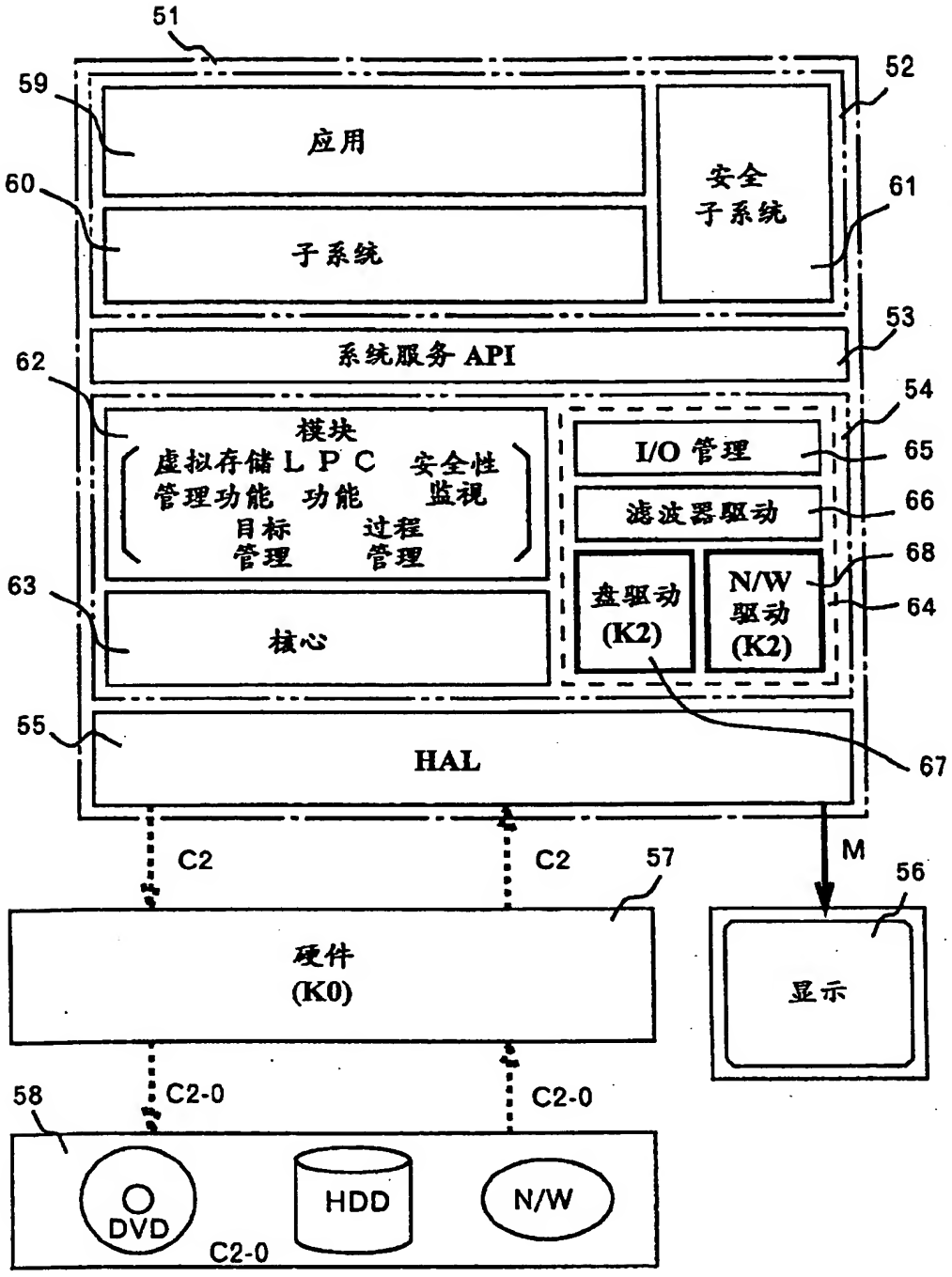

51
52
59
应用
安全
子系统
60
子系统
61
53
系统服务 API
62
54
模块
虚拟存储 LPC 安全性
管理功能 功能 监视
目标 过程
管理 管理
I/O 管理
65
滤波器驱动
66
68
盘驱动
(K2)
N/W
驱动
(K2)
64
63
核心
55
HAL
67
C2
C2
57
M
56
硬件
(K0)
显示
58
C2-0
C2-0
DVD
HDD
N/W
C2-0

图 7

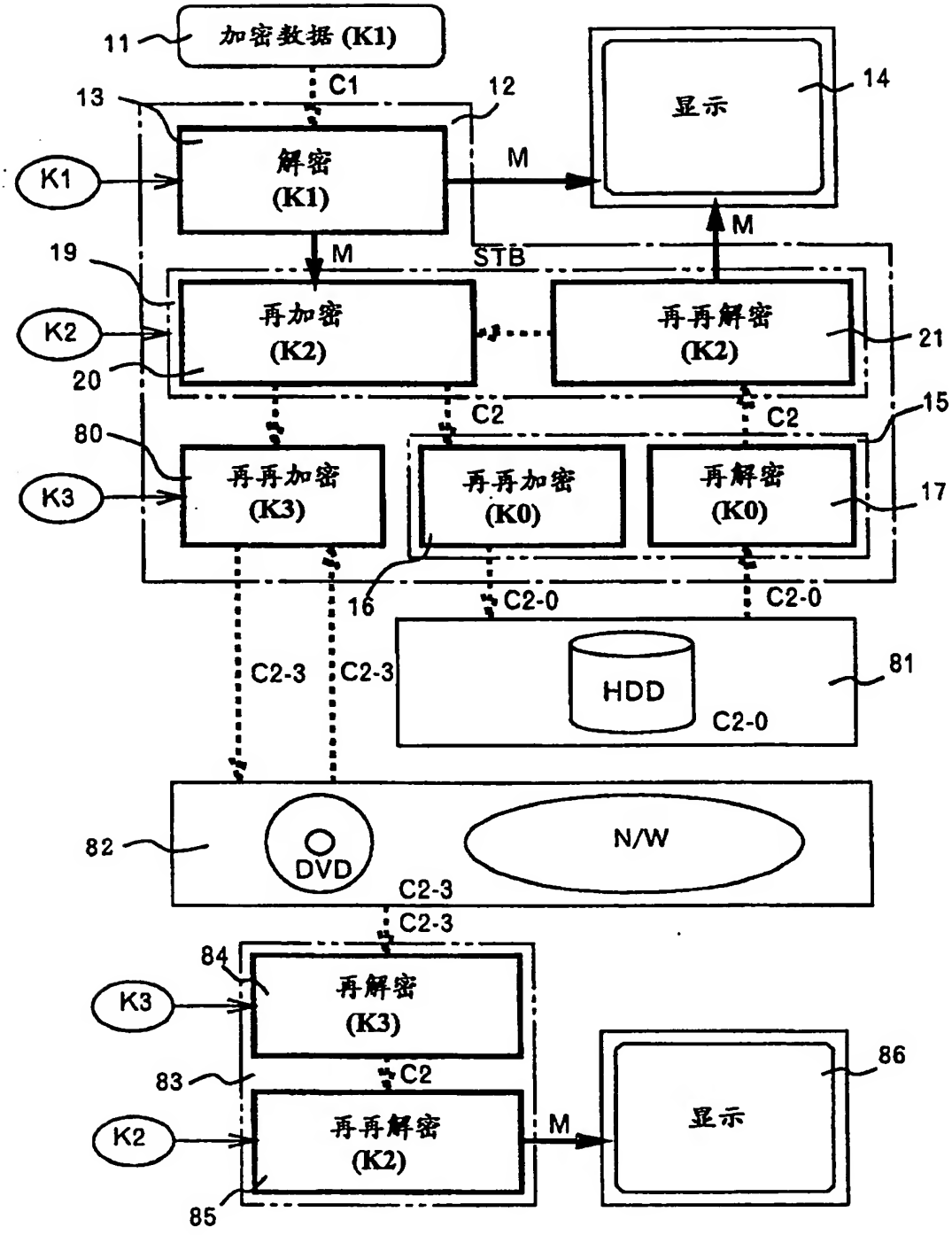

11
加密数据 (K1)
C1
13
12
显示
14
解密
(K1)
K1
M
M
M
STB
19
再加密
(K2)
K2
20
再再解密
(K2)
21
C2
C2
15
80
再再加密
(K3)
K3
再再加密
(K0)
再解密
(K0)
17
16
C2-0
C2-0
C2-3
C2-3
HDD
81
C2-0
82
DVD
N/W
C2-3
C2-3
84
再解密
(K3)
K3
C2
83
再再解密
(K2)
K2
M
显示
86
85

图 8

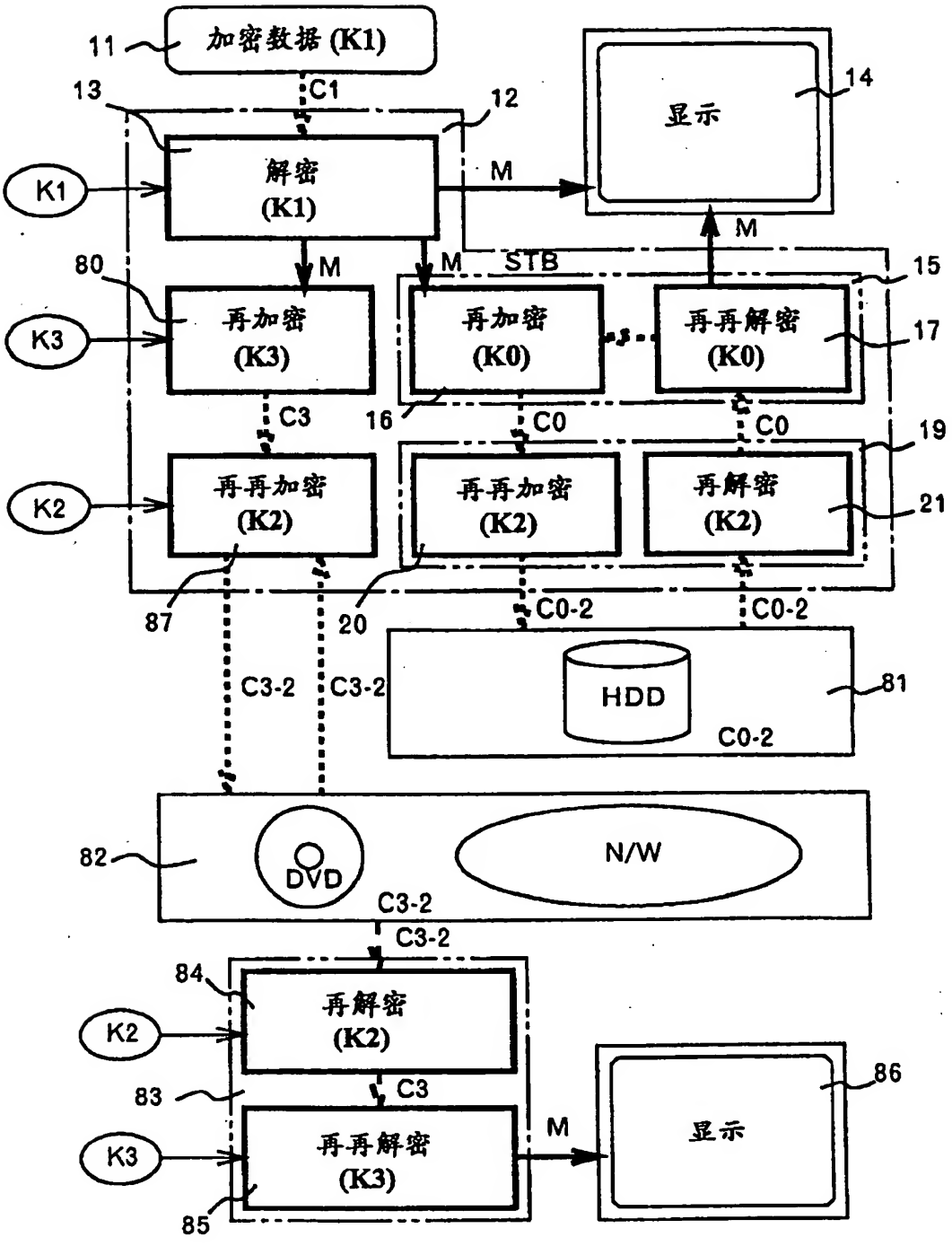

11
加密数据 (K1)
C1
13
12
显示
14
K1
解密
(K1)
M
M
M
STB
15
80
K3
再加密
(K3)
再加密
(K0)
再再解密
(K0)
17
C3
16
C0
C0
19
K2
再再加密
(K2)
再再加密
(K2)
再解密
(K2)
21
87
20
C0-2
C0-2
C3-2
C3-2
HDD
81
C0-2
82
DVD
N/W
C3-2
C3-2
84
K2
再解密
(K2)
C3
83
K3
再再解密
(K3)
M
显示
86
85

图 9

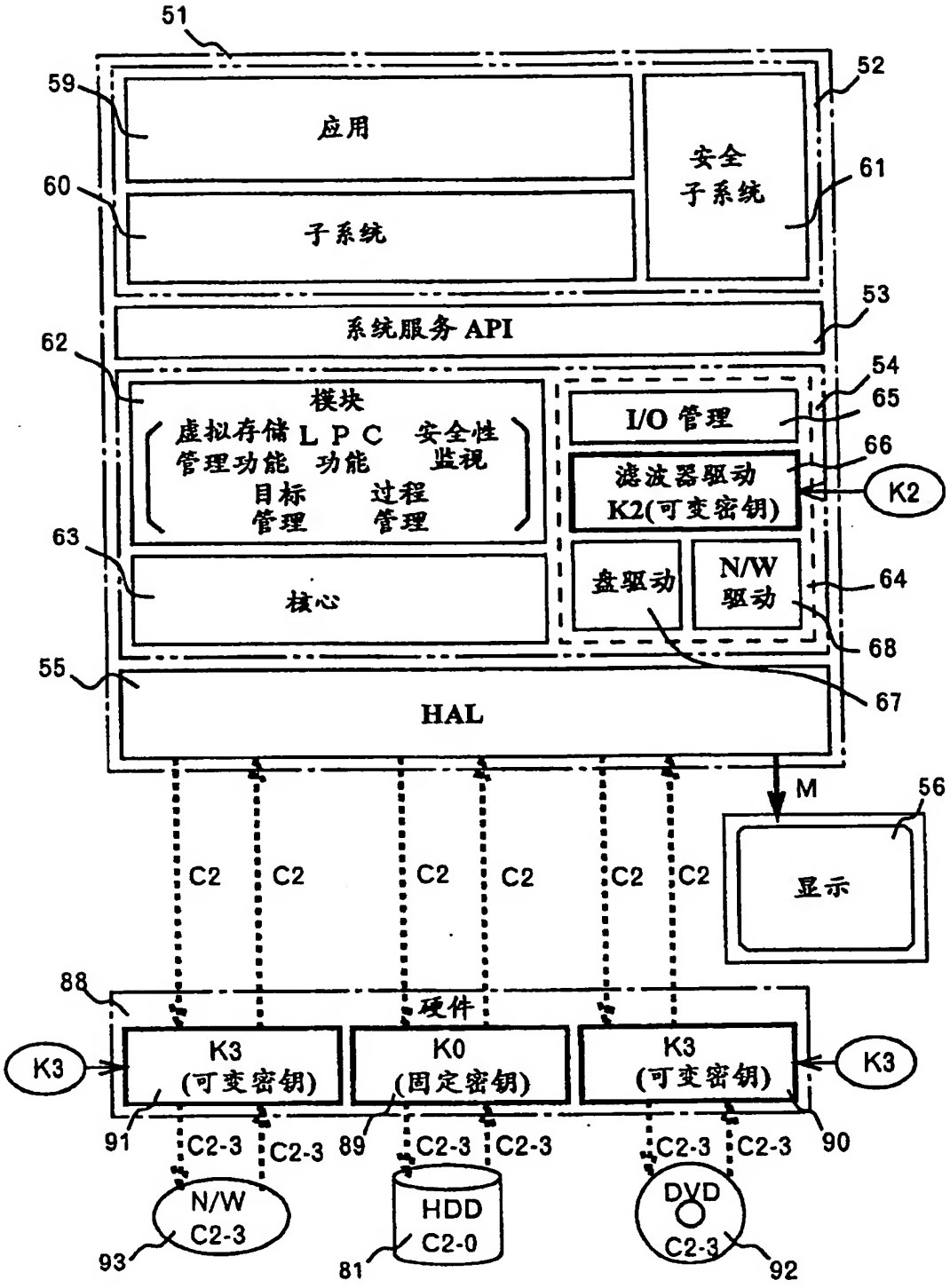

51
59
52
应用
安全
子系统
61
60
子系统
53
系统服务 API
62
54
模块
虚拟存储 管理功能
L P C 功能
安全性 监视
目标 管理
过程 管理
65
I/O 管理
66
滤波器驱动
K2(可变密钥)
K2
63
核心
盘驱动
N/W 驱动
64
68
55
67
HAL
M
56
显示
C2
C2
C2
C2
C2
C2
88
硬件
K3
K3
(可变密钥)
K0
(固定密钥)
K3
(可变密钥)
K3
91
C2-3
C2-3
89
C2-3
C2-3
C2-3
C2-3
90
N/W
C2-3
HDD
C2-0
DVD
C2-3
93
81
92

图 10

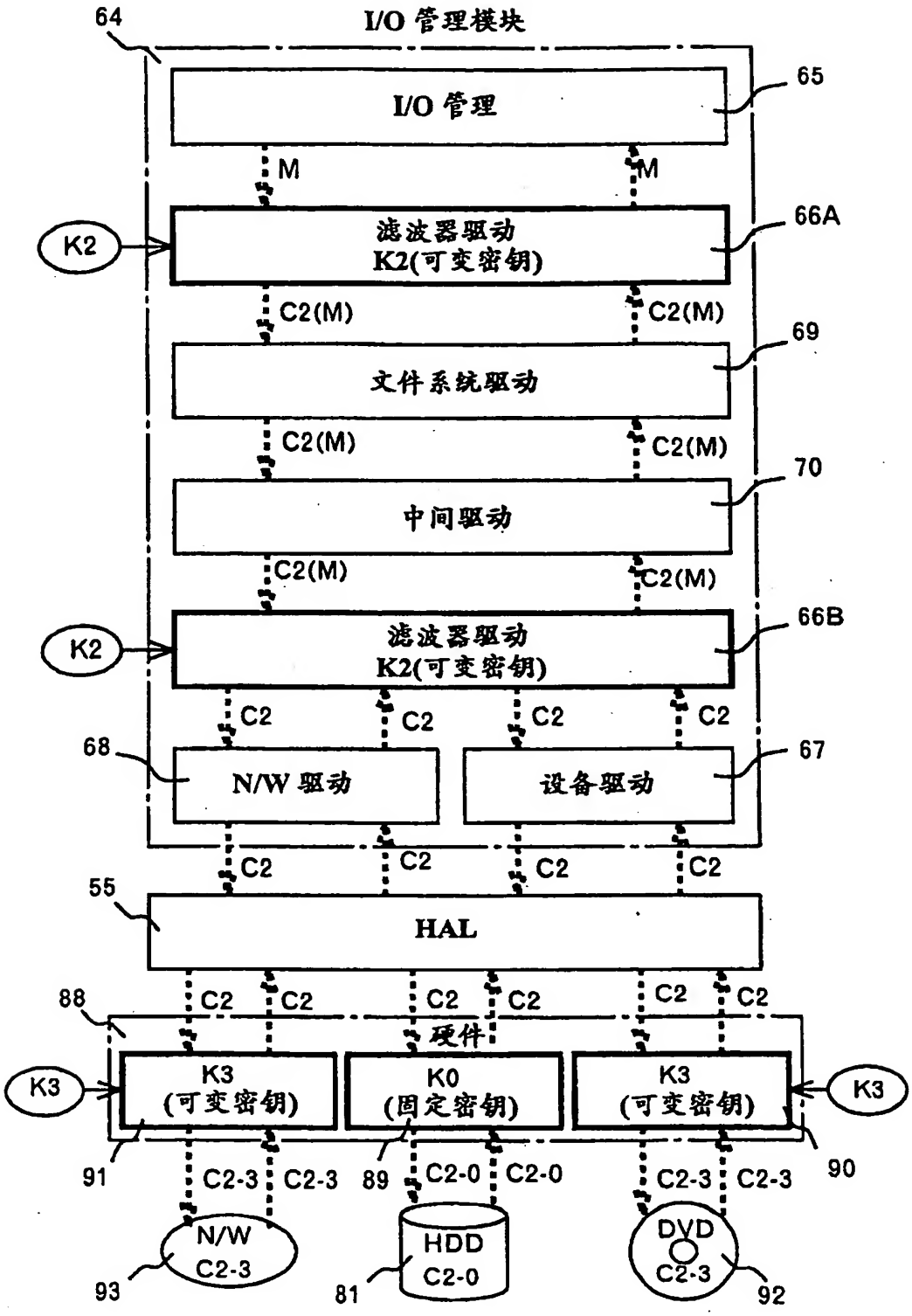

64
I/O 管理模块
I/O 管理
65
M
M
K2
滤波器驱动
K2(可变密钥)
66A
C2(M)
C2(M)
69
文件系统驱动
C2(M)
C2(M)
70
中间驱动
C2(M)
C2(M)
K2
滤波器驱动
K2(可变密钥)
66B
C2
C2
C2
C2
68
N/W 驱动
设备驱动
67
C2
C2
C2
C2
55
HAL
88
C2
C2
C2
C2
C2
C2
硬件
K3
K3
(可变密钥)
K0
(固定密钥)
K3
(可变密钥)
K3
91
89
90
C2-3
C2-3
C2-0
C2-0
C2-3
C2-3
N/W
C2-3
HDD
C2-0
DVD
C2-3
93
81
92

图 11

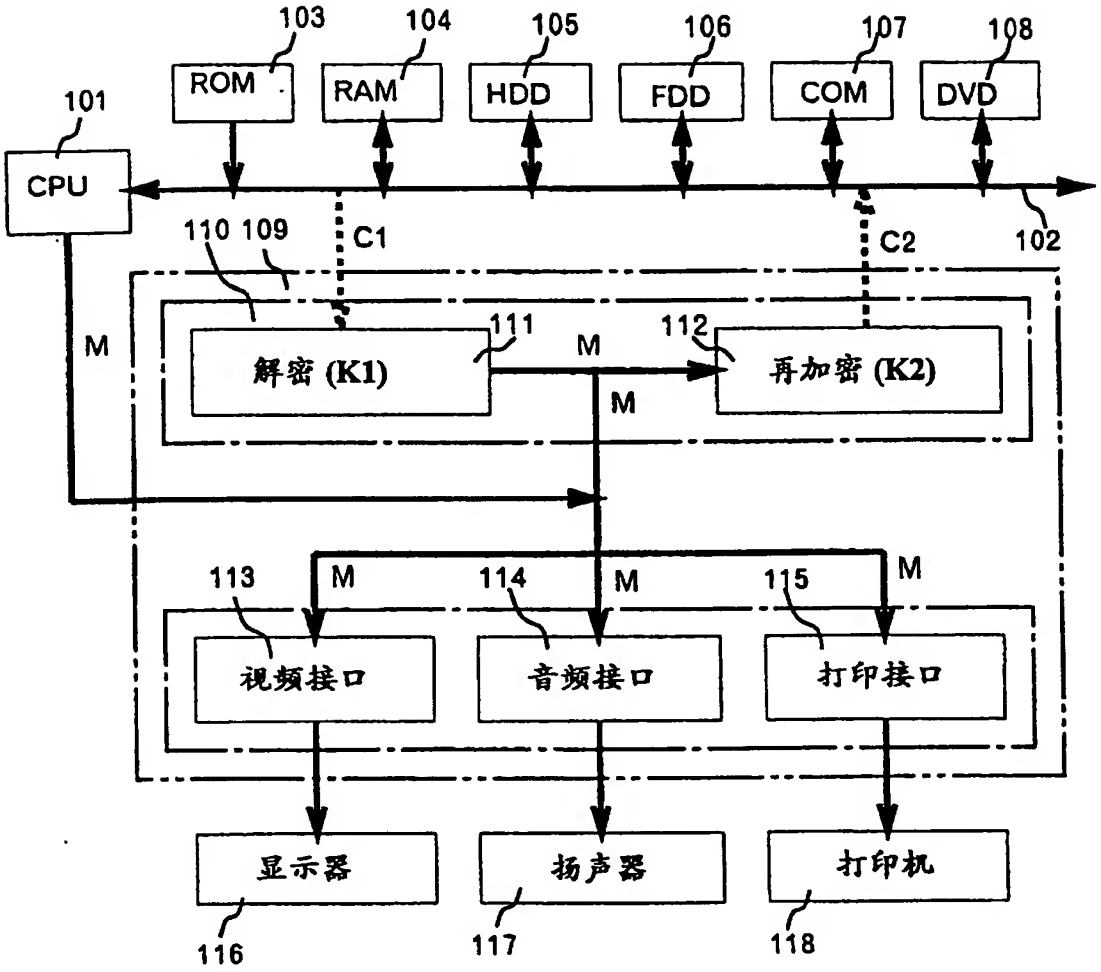

103
104
105
106
107
108
ROM
RAM
HDD
FDD
COM
DVD
101
CPU
110 109
C1
C2
102
M
111
112
解密 (K1)
M
再加密 (K2)
M
113
M
114
M
115
M
视频接口
音频接口
打印接口
显示器
扬声器
打印机
116
117
118

图 12

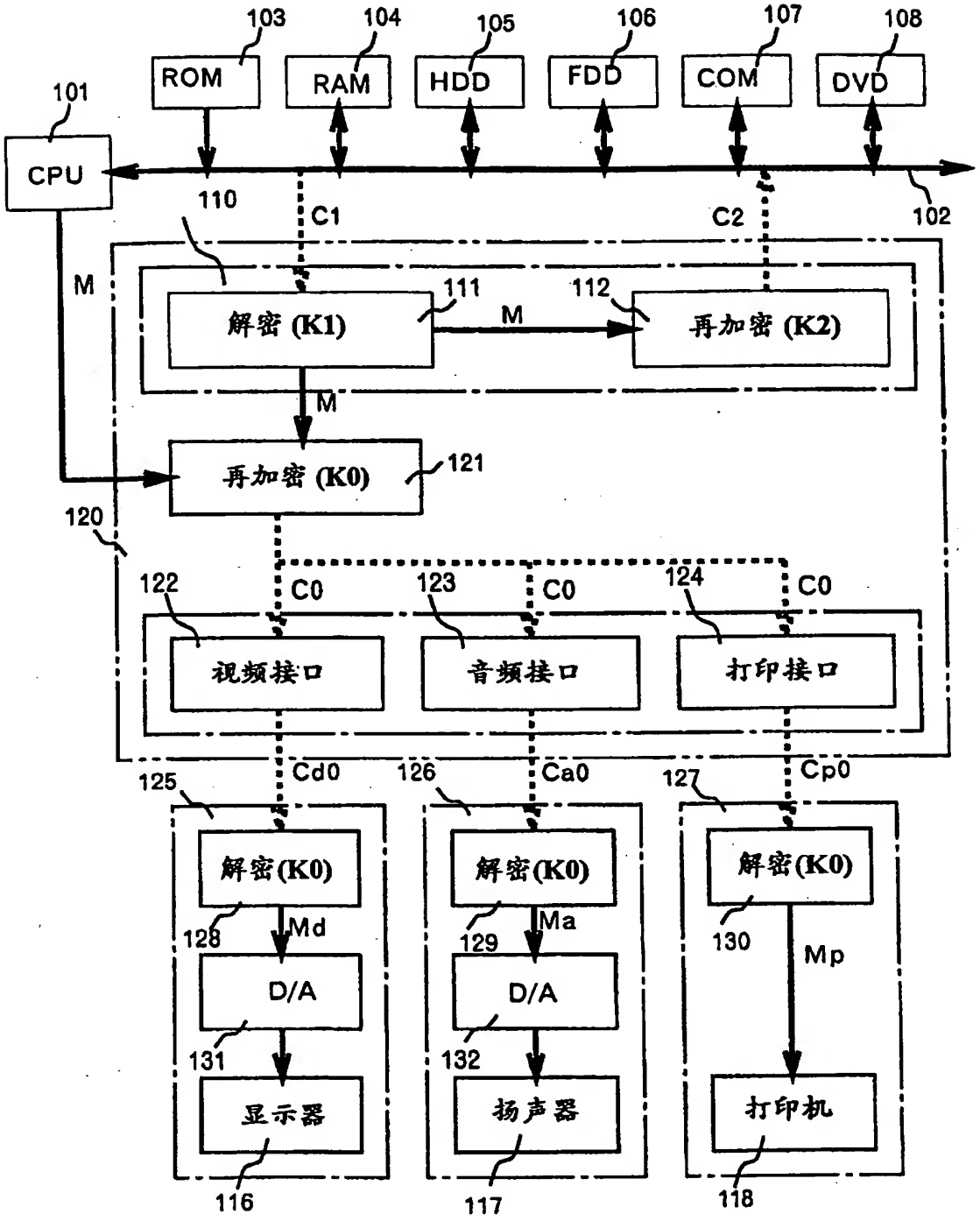

103
104
105
106
107
108
ROM
RAM
HDD
FDD
COM
DVD
101
CPU
110
C1
C2
102
M
111
112
解密 (K1)
M
再加密 (K2)
M
再加密 (K0)
121
120
122
C0
123
C0
124
C0
视频接口
音频接口
打印接口
125
Cd0
126
Ca0
127
Cp0
解密(K0)
解密(K0)
解密(K0)
128
Md
129
Ma
130
Mp
D/A
D/A
131
132
显示器
扬声器
打印机
116
117
118

图 13

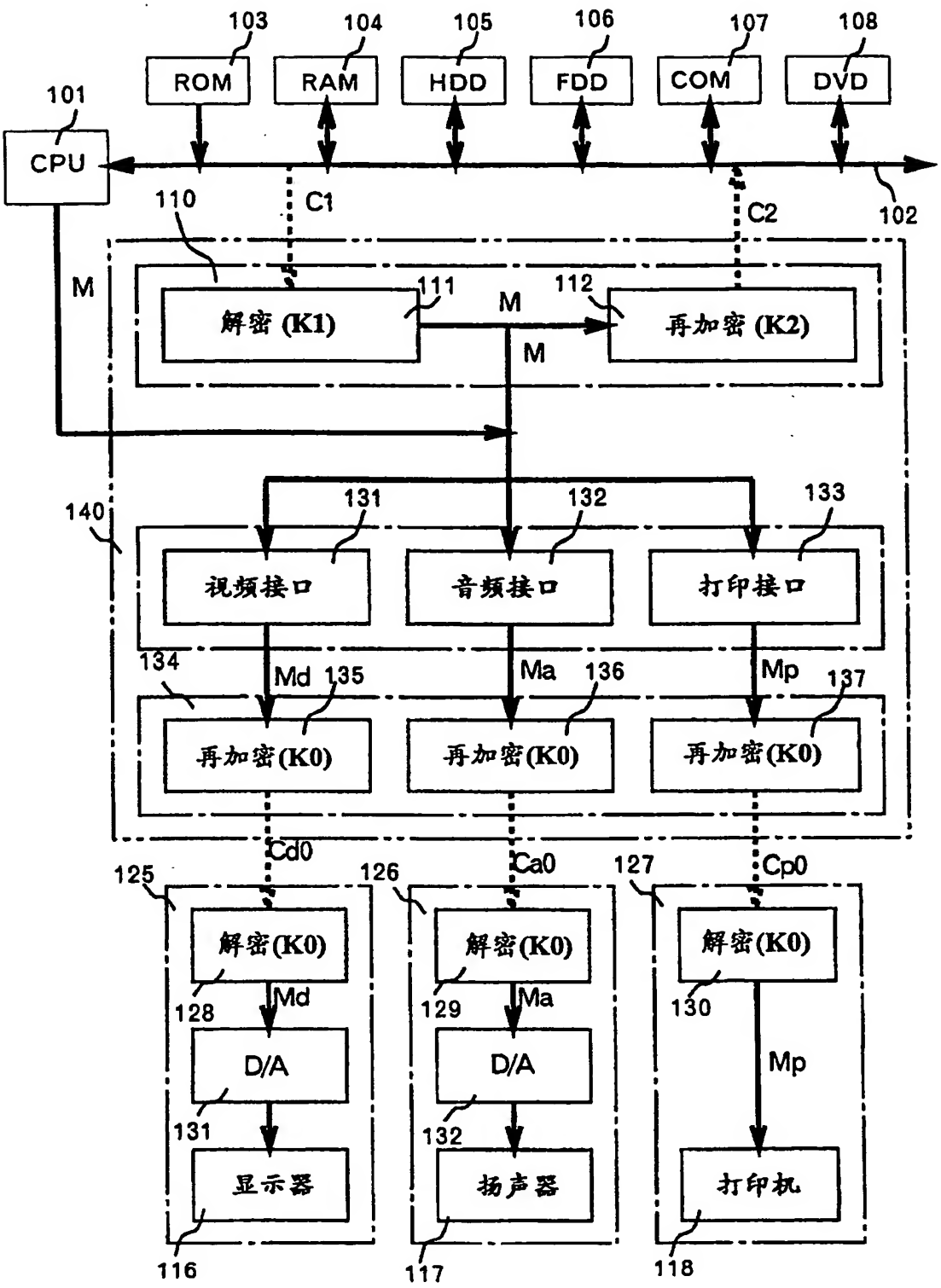

103
104
105
106
107
108
ROM
RAM
HDD
FDD
COM
DVD
101
CPU
C1
C2
102
110
M
111
112
解密 (K1)
M
M
再加密 (K2)
140
131
132
133
视频接口
音频接口
打印接口
134
Md
135
Ma
136
Mp
137
再加密(K0)
再加密(K0)
再加密(K0)
Cd0
Ca0
Cp0
125
126
127
解密(K0)
解密(K0)
解密(K0)
128
Md
129
Ma
130
Mp
D/A
D/A
131
132
显示器
扬声器
打印机
116
117
118

图 14